NAVAL POSTGRADUATE SCHOOL
Monterey, California

THESIS

POTENTIAL VULNERABILITIES OF A USMC TACTICAL WIRELESS LOCAL AREA NETWORK

by

John P. O'Sullivan

September 2001

Thesis Advisor:	John Osmundson
Associate Advisor:	Raymond Buettner

Approved for public release; distribution is unlimited.

Report Documentation Page

Report Date 30 Sep 2001	**Report Type** N/A	**Dates Covered (from... to)** -

Title and Subtitle Potential Vulnerabilities of a USMC Tactical Wireless Local Area Network	**Contract Number**
	Grant Number
	Program Element Number
Author(s) O?Sullivan, John P.	**Project Number**
	Task Number
	Work Unit Number
Performing Organization Name(s) and Address(es) Research Office Naval Postgraduate School Monterey, Ca 93943-5138	**Performing Organization Report Number**
Sponsoring/Monitoring Agency Name(s) and Address(es)	**Sponsor/Monitor's Acronym(s)**
	Sponsor/Monitor's Report Number(s)
Distribution/Availability Statement Approved for public release, distribution unlimited	
Supplementary Notes	
Abstract	
Subject Terms	
Report Classification unclassified	**Classification of this page** unclassified
Classification of Abstract unclassified	**Limitation of Abstract** UU
Number of Pages 91	

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE	*Form Approved OMB No. 0704-0188*

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.

1. AGENCY USE ONLY *(Leave blank)*	**2. REPORT DATE** September 2001	**3. REPORT TYPE AND DATES COVERED** Master's Thesis

4. TITLE AND SUBTITLE: Title (Mix case letters) Potential Vulnerabilities of a USMC Tactical Wireless Local Area Network	**5. FUNDING NUMBERS**
6. AUTHOR O'Sullivan, John P.	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000	**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A	**10. SPONSORING / MONITORING AGENCY REPORT NUMBER**

11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for Public Release; distribution is unlimited	**12b. DISTRIBUTION CODE**

13. ABSTRACT ***(maximum 200 words)***

As part of the ongoing Revolution in Military Affairs, the Navy and Marine Corps are engaged in an ambitious effort to integrate emerging technologies into new operational concepts. The vision of future conflict places heavy emphasis on highly mobile forces that will require unprecedented cooperation between forces afloat and ashore. These new operational concepts, such as Operational Maneuver From the Sea (OMFTS), require new technologies to give small combat units unmatched situational awareness ultimately leading to greater combat power. The Extending the Littoral Battlespace (ELB) Advanced Concept Technology Demonstration has sought to demonstrate new advances in joint expeditionary warfare significantly aided by a commercial-off-the-shelf wireless communications system.

This thesis examines potential vulnerabilities of the ELB wireless local area network. Specifically, it explores the impact such vulnerabilities may have on the eventual ability of supported units to accomplish their mission in an OMFTS-type scenario. The vulnerabilities are divided between the two network layers defined by the commercial standard, the physical and MAC layers. This study concludes that there are considerable vulnerabilities at both network layers, the most significant for a military application, however, are those associated with the physical layer and therefore alternate physical layer solutions should be sought for tactical wireless networks of the future.

14. SUBJECT TERMS Wireless Networks, IEEE 802.11, ELB, Information Superiority, WARNET, Operational Maneuver From The Sea	**15. NUMBER OF PAGES** 91
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UL

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

POTENTIAL VULNERABILITIES OF A USMC TACTICAL WIRELESS LOCAL AREA NETWORK

John P. O'Sullivan
Commander, United States Navy
B.S., U.S. Naval Academy, 1984

Submitted in partial fulfillment of the
requirements for the degree of

**MASTER OF SCIENCE IN
INFORMATION TECHNOLOGY MANAGEMENT**

from the

**NAVAL POSTGRADUATE SCHOOL
September 2001**

Author: John P. O'Sullivan

Approved by: John S. Osmundson
John Osmundson, Thesis Advisor

Raymond Buettner, Associate Advisor

Dan C Boger
Dan C. Boger, Chairman
Information Systems Academic Group

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

As part of the ongoing Revolution in Military Affairs, the Navy and Marine Corps are engaged in an ambitious effort to integrate emerging technologies into new operational concepts. The vision of future conflict places heavy emphasis on highly mobile forces that will require unprecedented cooperation between forces afloat and ashore. These new operational concepts, such as Operational Maneuver From the Sea (OMFTS), require new technologies to give small combat units unmatched situational awareness ultimately leading to greater combat power. The Extending the Littoral Battlespace (ELB) Advanced Concept Technology Demonstration has sought to demonstrate new advances in joint expeditionary warfare significantly aided by a commercial-off-the-shelf wireless communications system.

This thesis examines potential vulnerabilities of the ELB wireless local area network. Specifically, it explores the impact such vulnerabilities may have on the eventual ability of supported units to accomplish their mission in an OMFTS-type scenario. The vulnerabilities are divided between the two network layers defined by the commercial standard, the physical and MAC layers. This study concludes that there are considerable vulnerabilities at both network layers, the most significant for a military application, however, are those associated with the physical layer and therefore alternate physical layer solutions should be sought for tactical wireless networks of the future.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

I. INTRODUCTION 1
- A. OVERVIEW 1
- B. PURPOSE 2
- C. THESIS OUTLINE 3
- D. EXPECTED BENEFITS OF THIS THESIS 3

II. BACKGROUND 5
- A. DOCTRINAL WRITINGS 5
  - 1. …From the Sea 5
  - 2. Joint Vision 2010 6
    - *a. Information Superiority 7*
  - 3. Operational Maneuver from the Sea (OMFTS) 8
- B. ADVANCED CONCEPT TECHNOLOGY DEMONSTRATIONS (ACTD) 10
- C. COMMERCIAL-OFF-THE-SHELF (COTS) 11
  - 1. Advantages of COTS 12
  - 2. Disadvantages of COTS 12

III. WIRELESS NETWORKS 15
- A. INTRODUCTION 15
- B. WIRELESS LOCAL AREA NETWORKS 15
- C. IEEE 802.11 STANDARD 17
- D. NETWORK TOPOLOGY 19
  - 1. Station 19
  - 2. Basic Service Set 19
  - 3. Extended Service Set 20
    - *a. Distribution System 21*
- E. IEEE 802.11 PHYSICAL LAYER 22
  - 1. Direct Sequence Spread Spectrum 23
- F. IEEE 802.11 MEDIUM ACCESS CONTROL LAYER 25
  - 1. Basic Access Mechanism 26
    - *a. Point Coordination Function (PCF) 27*
  - 2. Distribution Services 27
  - 3. Privacy 29

IV. EXTENDING THE LITTORAL BATTLESPACE ACTD 31
- A. BACKGROUND 31
- B. ELB ACTD OBJECTIVES 32
  - 1. Communications and Networking 33
  - 2. Command and Control 33
  - 3. Fires and Targeting 33
  - 4. Sensors and Intelligence 34
- C. ELB COMMUNICATIONS 34
  - 1. Communications Architecture 35
    - *a. Tier 1 .... 37*

b. *Tier 2* ... 39
c. *Tier 3* ... 40

V. POTENTIAL VULNERABILITIES ... 41
A. **INTRODUCTION** ... 41
1. **Information Warfare and Vulnerability** ... 41
a. *ELB Communications* ... 42
B. **DETECTION** ... 44
1. **LPD/LPI** ... 45
a. *IEEE 802.11b* ... 46
b. *ELB WLAN* ... 49
C. **JAMMING** ... 49
1. **Jamming IEEE 802.11b** ... 51
a. *ELB WLAN* ... 55
D. **EXPLOITATION** ... 57
1. **IEEE 802.11b** ... 58
a. *Authentication* ... 58
b. *WEP* ... 61
2. **ELB WLAN** ... 63
a. *EUT Capture* ... 64

VI. CONCLUSION ... 65
A. **SUMMARY OF VULNERABILITIES** ... 65
1. **Physical Layer** ... 65
2. **MAC Layer** ... 66
B. **IMPACT OF ELB VULNERABILITIES ON OMFTS** ... 66
C. **RECOMMENDATIONS** ... 68

LIST OF REFERENCES ... 73

INITIAL DISTRIBUTION LIST ... 77

TABLE OF FIGURES

Figure 1. Emerging Operational Concepts [From: 7] 7
Figure 2. Maneuver Warfare [From: 6].......... 9
Figure 3. IEEE 802.11 standards mapped to OSI reference model [From: 13] 18
Figure 4. Basic Service Set [From: 13] 20
Figure 5. Infrastructure Basic Service Set [After: 13] 20
Figure 6. Extended Service Set [From: 13] 21
Figure 7. Industrial, Scientific, and Medical Bands [From: 14] 22
Figure 8. Maximum Allowable Transmit Power [From: 12] 23
Figure 9. DSSS Channels [After: 12] 23
Figure 10. DSSS Modulation with 11-bit Barker sequence [After: 12] 25
Figure 11. Hidden Node Problem 27
Figure 12. Relationship between State Variables and Services [From: 12] 28
Figure 13. Privacy Pyramid 30
Figure 14. ELB MSD-2 Architecture [After: 18] 36
Figure 15. End User Terminal [After: 18] 37
Figure 16. Communications Vehicle Schematic [After: 18] 38
Figure 17. Tier 3 Architecture [After: 18] 40
Figure 18. IW Scenario [After: 20] 43
Figure 19. Low Power Density 45
Figure 20. *Eb*/*No* vs. BER 48
Figure 21. DSSS throughput vs. Interference-to-Signal Ratio [From: 25] 52
Figure 22. J/S vs. Data Rate [From: 25] 54
Figure 23. Star Topography 56
Figure 24. MAC Management Frame Format [From: 12] 59
Figure 25. UWB Advances [From: 31] 69

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

Table 1. Principles of Operational Maneuver from the Sea 9
Table 2. ACTD Consideration Factors 11
Table 3. WLAN Benefits 16
Table 4. WLAN Standards 17
Table 5. Characteristics of Spread Spectrum Signals [After: 16] 24
Table 6. USCINCPAC Critical Operational Issues [After: 3] 32
Table 7. Desired Qualities of ELB WLAN [From: 3] 35
Table 8. Comparison of 1Mbps and 11Mbps AJ Margins 53

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. OVERVIEW

As we stand now at the beginning of the 21st century there is little debate that we find ourselves in the midst of a Revolution in Military Affairs (RMA). According to the Office of the Secretary of Defense, "A Revolution in Military Affairs is a major change in the nature of warfare brought about by the innovative application of new technologies which, combined with dramatic changes in military doctrine and operational and organizational concepts fundamentally alters the character and conduct of military operations." [1] It is certainly not by coincidence that this RMA is taking place concurrently with an information revolution; rather it is a direct result of this information revolution. We have entered into the "Information Age", where information systems permeate our military and civilian lives, and are central to the way we will conduct future operations. It is clear that the innovative application of new information technologies is providing the opportunity for dramatic changes in military doctrine that is required to sustain the current RMA. Two changes that characterize the current RMA, dramatically improved command and control (C2) functions and information warfare (IW), have a direct link to the information revolution. [2] Similar to the RMA that occurred in the 1930's prior to World War II, this is all taking place during a period of cutbacks in military spending. This fact, combined with the unprecedented advancements of information technologies in the civilian sector, has lead the Department of Defense (DoD) to look to commercial-off-the-shelf (COTS) systems in its attempt to keep pace with the information revolution and consequently, the RMA.

It is within this environment that the Navy and Marine Corps have engaged in an ambitious effort to integrate emerging technologies into new operational concepts. Building on the foundation laid by the white paper "From the Sea" the Marine Corps published its concept paper, "Operational Maneuver from the Sea". Both of these documents provide a vision of future conflict that places heavy emphasis on the littoral regions of the world, with highly mobile forces requiring unprecedented cooperation between forces afloat and ashore. The operational concept of information superiority is the foundation upon which Joint Vision 2010 (JV 2010) is based. Information superiority is not viewed necessarily as an enabler, but rather as a prerequisite to operate according to this vision. The significant enhancements in communications and information management required by such a vision can only be possible through the incorporation of new information technologies.

The Extending the Littoral Battlespace (ELB) Advanced Concept Technology Demonstration (ACTD) is a joint demonstration being conducted by the Navy and Marine Corps that supports key elements of JV 2010. The ELB ACTD, sponsored by the Commander-in-Chief, U.S. Pacific Command, (CINCPAC) seeks to demonstrate and assess the military utility of communication technology and operational procedures that enable seamless operations by joint expeditionary forces in the world's littoral areas. [3] A primary focus of this demonstration is to achieve information superiority through network-centric operations all the way down to the tactical level, or in communications terminology, "the last mile". To this end, a tactical wireless local area network (WLAN), compliant with the IEEE 802.11 standard and composed primarily of COTS components, is being evaluated based on its ability to enable a flattened informational structure that will support small combat units ashore.

B. PURPOSE

The intent of this thesis is to evaluate the ELB WLAN for potential vulnerabilities that may detract from its stated purpose of supporting small combat units ashore. It will take a systems level view of the current ELB WLAN and, in the context of the RMA and JV 2010, assess whether it is an innovative application of new technology that can support fundamental changes in military doctrine. More specifically, this thesis will explore the concept of information superiority in some detail and attempt to determine if the vulnerabilities of the ELB WLAN could potentially contribute to the eventual failure to achieve the desired state of information superiority. Since the concept of "vulnerability" is central to this thesis it is important to properly define it. As used in this thesis, a vulnerability of a system is any characteristic that causes it to suffer a definite degradation, loss or reduction of capability, as a result of being subjected to a certain level of effects in a hostile military environment. [4] With this definition in mind, this thesis will not address technical implementation issues, such as roaming, that are still being studied in order to optimize wireless systems performance. This thesis serves as a follow on to a previous work completed in June 2000 titled, "Scalability Study of Wireless Tactical Communications in Support of a Marine Corps Expeditionary Brigade." The previous thesis focused on the technological feasibility and the infrastructure needed to support a wireless network as envisioned by the ELB ACTD. It was demonstrated, through modeling, that current technology could be used to develop such a wireless network. Technological feasibility, however, should be only one step in a long process of evaluating the military utility of current wireless technology.

C. THESIS OUTLINE

Following this introduction, Chapter II will contain a literature review of pertinent doctrinal writings that formulate the vision of future Navy-Marine Corps operations and the central role that information superiority, and therefore communications, will assume. Because of its close association with JV 2010, a description and objectives of the ACTD program will be included. This chapter will also include a discussion on the use of COTS systems and components in DoD information systems. So as to lay a foundation for a discussion of the ELB WLAN, Chapter III will cover the fundamentals of wireless networks, with specific focus on the IEEE 802.11 standard. Although this thesis assumes a systems level view of the ELB WLAN, a certain level of technical discussion is presented to lead into later vulnerability issues. Chapter IV will be a description of the ELB ACTD, including the objectives and specific network components, as well as network implementation issues. Chapter V is a discussion of potential vulnerabilities and impacts such vulnerabilities may have on the intended mission of the network. Finally, the conclusions will be provided in Chapter VI.

D. EXPECTED BENEFITS OF THIS THESIS

For the past decade the promise of wireless solutions has been a major focus of commercial technology development. Without question the freedom of mobility that wireless products promise will have tremendous impacts both in the commercial and defense sectors. As the first two generations of wireless products have already hit the market and the third is about to, there has been a significant amount of research on the vulnerabilities of such products. Rather than continue along the lines of identifying additional vulnerabilities, this thesis will attempt to take the next step and identify how such identified vulnerabilities will impact the military utility of one such wireless solution. The potential benefit to the ELB program specifically is that it provides an independent evaluation of whether its network will fulfill its mission. More generally, however, this thesis may motivate ensuing students to continue work in bridging the gap between technical solutions and operational concepts.

II. BACKGROUND

A. DOCTRINAL WRITINGS

It is helpful to review pertinent doctrinal writings to facilitate an understanding of how a communication system, such as a WLAN, can be a critical component in the vision of future warfare. These writings illustrate how the anticipated increased access to information is critical to the ultimate success of operational concepts such as extending the littoral battlespace. It is important to point out that many these writings were completed in the aftermath of the Gulf War and the demise of the Cold War, in an environment of significant military personnel reductions and budget cuts. Rather than continue with the same operational concepts that were so successful only a few short years prior it became clear that the environment in which future operations would occur would be drastically different and the number of forces to carry out such operations would be radically reduced. In these writings one notices an increasing emphasis upon mobility of forces, and away from strength-on-strength engagements; which ultimately requires greater capabilities in command, control, communications, computers, and intelligence (C4I) systems and thus increases the value of information exchange.

1. …From the Sea

Published in 1992, this Navy and Marine Corps White Paper set the stage for the strategic concept intended to carry the Naval Service beyond the Cold War and into the 21st century. No longer would the primary focus of naval strategy be on a global threat but rather in the future it would focus on regional challenges. While the prospect of global war receded, we entered into a period of uncertainty in regions critical to our national security. This change in strategic direction represented a fundamental shift away from an open-ocean, or blue water, naval strategy to one that is focused upon the complex operating environment in the littoral regions of the world. [5] Although composing only a small portion of the earth's surface, the littorals contain over 80 percent of the earth's population, as well as nearly all the marketplaces for international trade. [6]

2. Joint Vision 2010

Just as the Navy and Marine Corps did in **"…From the Sea"**, the Army and Air Force each published separate visions of their respective strategic role in the nation's defense. What was clearly missing was a unified vision of joint warfare in the future. First introduced in 1996, JV 2010 filled that void by laying out a conceptual template for, among other things, leveraging technological opportunities to achieve new levels of effectiveness in joint warfighting. This document provides a common direction for the Services in developing their unique capabilities within a joint framework. It reiterates that accelerating rates of global change will make the future environment much less stable and therefore unpredictable. Continued rapid technological advances will have significant impact on military forces and failure to adopt such technologies could increase future risks. For the United States does not have a monopoly on such technological advances, but rather wider access will make such technology available to potential adversaries. Specifically, exponential improvements in information technologies will significantly impact future military operations by providing decision makers with accurate information in a timely manner. Forces that are able to capitalize on these capabilities will gain dominant battlespace awareness. They will be able to successfully attack targets with fewer platforms while achieving objectives more rapidly and with reduced risks. JV 2010 first introduced the concept of "full spectrum dominance" which it maintained would be achieved through four operational concepts: dominant maneuver, precision engagement, full dimensional protection, and focused logistics. Ultimately the objective is to achieve massed effects from more dispersed forces. [7]

These operational concepts are the cornerstone of JV 2010. Dominant maneuver is the "multidimensional application of information, engagement, and mobility capabilities to position and employ widely dispersed joint air, land, sea and space forces to accomplish the assigned operational tasks." Precision engagement is "a system of systems that enables our forces to locate the objective or target, provide responsive C2, generate the desired effect, assess our level of success, and retain the flexibility to re-engage with precision when required." Full-dimensional protection is the "multi-layer capability to better protect our forces and centers of gravity at all levels from adversary attacks while maintaining freedom of action during deployment, maneuver and engagement." Focused logistics is the "fusion of information, logistics, and transportation technologies to provide rapid crisis response, to track and shift assets even while en route, and to deliver tailored logistics packages and sustainment directly at the strategic, operational, and tactical level of operations." [7]

a. Information Superiority

The most critical operational concept introduced in JV 2010, however, is information superiority. As illustrated in Figure 1, it is the foundation upon which the four other operational concepts are based. JV 2010 defines information superiority as, "The capability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same." [7]

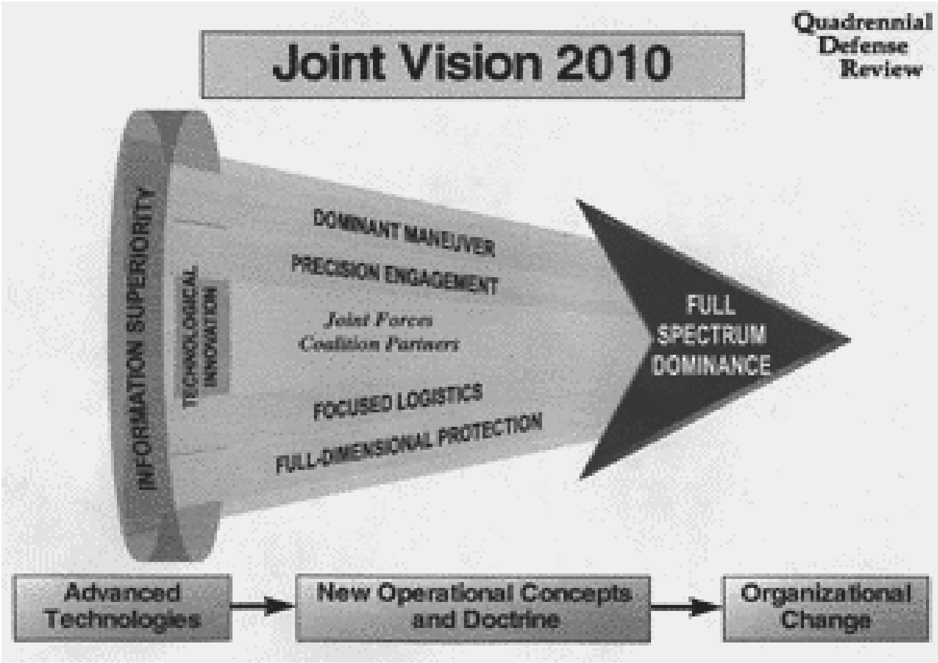

Figure 1. Emerging Operational Concepts [From: 7]

JV 2010 does not merely suggest that information superiority is a desired state, but rather affirms specifically "we must have information superiority." [7] So rather than viewing information superiority as a "capability" it is more appropriate to view it as a "condition" that must be met prior to employing the four other operational concepts to ultimately gain full spectrum dominance. This is analogous to requiring the condition of achieving air or sea dominance prior to committing the main body of an attack. There is little doubt that our attempts to achieve information superiority will be meet with opposition. In fact a weaker adversary may recognize early that denial of this state may be its only chance of victory. IW is a logical means to both, achieve information superiority for oneself and deny an adversary's attempt to achieve information superiority. Offensive IW degrades an adversary's collection or use of information, while defensive IW is required to protect our own ability to maintain an uninterrupted flow of information. The cornerstone of information superiority is advanced C4I systems, which can provide to all tactical levels of command a robust, continuous, common operating picture of the battlespace. As envisioned in JV 2010, this significantly increased information flow will give warfighters at the individual or small unit levels significant advantage over an enemy. Through increased situational awareness (SA) of the operational environment they will be able to make better decisions more rapidly, without relying upon direction from higher headquarters. [7] If in fact information superiority is a condition for mission success then the next logical quandary for commanders is trying to determine if and when it has been achieved. Currently there is no clear-cut means of measuring information superiority.

3. Operational Maneuver from the Sea (OMFTS)

Published in 1997, OMFTS expanded upon the movement towards unprecedented emphasis on littoral areas, requiring more intimate cooperation between forces afloat and ashore, that was first introduced in **…From the Sea**.

> OMFTS is a response to both danger and opportunity. The danger, summarized by the phrase "chaos in the littorals," consists of a world characterized by the clash of the myriad forces of national aspiration, religious intolerance, and ethnic hatred. The opportunity comes from significant enhancements in information management, battlefield mobility, and the lethality of conventional weapons. [6]

Consistent with JV 2010, OMFTS places heavy importance on new technologies to give small units unprecedented combat power. And because small units move more quickly than large ones they will possess the ability to conduct operations at a tempo significantly higher than ever before. Table 1 lists the guiding principles of OMFTS.

- Focus on an operational objective
- Use the sea as maneuver space
- Generate overwhelming tempo and momentum
- Pit strength against weakness
- Emphasize intelligence, deceptions, and flexibility

Table 1. Principles of Operational Maneuver from the Sea

The emphasis on small units will significantly reduce the infrastructure that will be required when a landing force arrives ashore. Rather than requiring a large logistics trail to be established prior to advancing towards the objective, the landing force will be largely self-contained and can therefore move toward the objective with speed, free of logistical constraints. Figure 2 illustrates how the elimination of the need to take a large beachhead to serve as a logistics hub will provide greater opportunity for a commander to move his units directly from the ship to its objective.

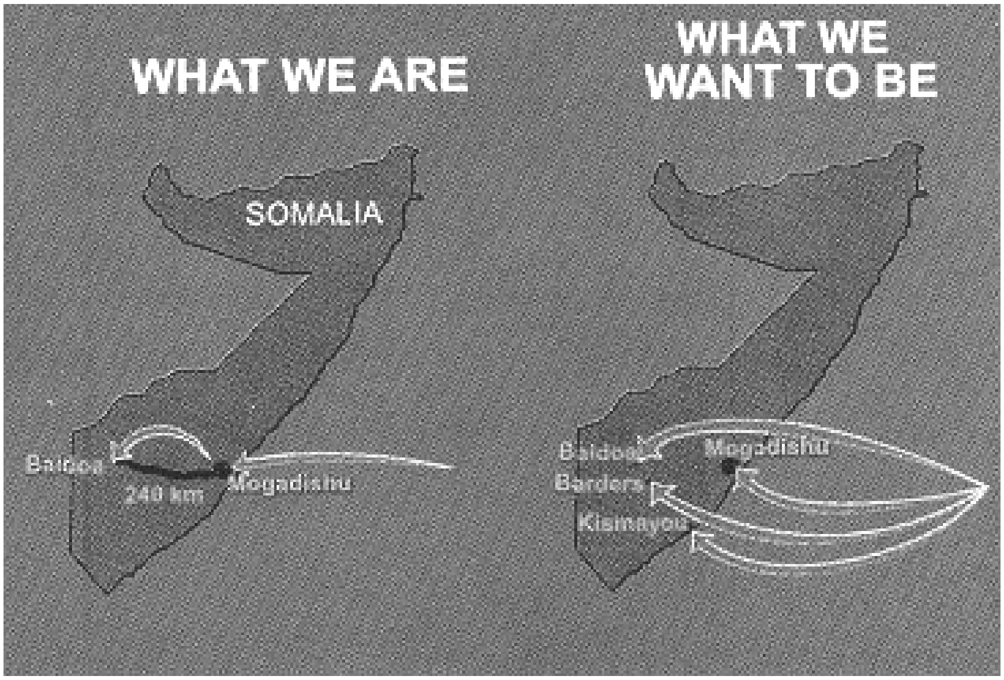

Figure 2. Maneuver Warfare [From: 6]

A considerable portion of the infrastructure in the past has been the necessary C4I systems required to maintain the flow of information between ships and the units ashore. It is due to this requirement that OMFTS identified C2 as being one area requiring considerable capability improvement in order to move from a conceptual framework into operational practice.

> The command and control system best suited to OMFTS will be very different from those developed to deal with previous approaches to amphibious warfare. Techniques previously employed to compensate for the inability of fire support units to see the battlefield will give way to techniques that exploit the fact that combatant units will be better informed than ever before. Communications systems designed to provide a few headquarters with an overall view of the situation will have to be replaced by those that provide units with control over the information they need. [6]

This is particularly noteworthy because it focuses information superiority all the way down to the tactical level. The projected new capabilities will enable tactical commanders to make decisions as the situation develops rather than relying upon information from the rear. Lieutenant General Paul Van Riper commented before a congressional subcommittee, “Our goal is to equip every Marine with the ability to win on the battlefields of the 21st century, where the junior enlisted Marine may well need and use more information than a battalion commander does today.” [8]

B. ADVANCED CONCEPT TECHNOLOGY DEMONSTRATIONS (ACTD)

> ACTDs exploit mature and maturing technologies to solve important military problems. A declining budget, significant changes in threats, and an accelerated pace of technology development have challenged our ability to adequately respond to evolving military needs. [9]

The ACTD program is a joint effort by the acquisition and operational communities designed to allow users to gain an understanding of proposed new capabilities. It was first initiated in 1994 with the goal to provide a prototype capability to the operator and to support the evaluation of that capability. ACTDs emphasize technology assessment and integration in response to validated military needs rather than technology development. This is in contrast to advance technology demonstrations, which are intended to evolve and demonstrate new technologies. The objective of an ACTD is to provide decision-makers an opportunity to fully understand the operational potential offered by a proposed new military capability before making an acquisition decision. The warfighter develops operational concepts designed to exploit the proposed capability, and then uses prototypes in realistic military exercises to assess the resulting military utility. At the completion of an ACTD, the residual systems used in the evaluation process are left with the user to provide limited operational capability. [9] Table 2 lists four critical factors that must be considered during the ACTD formulation phase.

- Affordability
- Interoperability
- Sustainability
- Evolutionary capability

Table 2. ACTD Consideration Factors

C. COMMERCIAL-OFF-THE-SHELF (COTS)

A discussion of COTS products is apposite on the basis that the fundamental technology behind a significant majority of ACTDs is currently being used in COTS products. This is quite natural given the requirement that only “mature or maturing” technologies be considered for ACTDs. Additionally, a review of the four critical review factors listed in Table 2 argues for the incorporation of COTS components in developing systems with military utility. There is little question that the concept of information superiority is in fact a product of the information technologies explosion in the commercial sector that has occurred in recent years and that JV 2010 clearly intended to leverage this for military applications.

> We will need a responsive research, development, and acquisition process to incorporate new technologies. This process must leverage technology and management innovations originating in the private sector through responsive access to commercial developments. [7]

Even prior to the publication of JV 2010 there was a strong movement towards the incorporation of COTS products in defense systems. In 1994, then Secretary of Defense William Perry signed a memorandum "Specifications and Standards – A New Way of Doing Business" which significantly changed the defense acquisition process. This policy directed the use of performance and commercial specifications and discouraged the use of military specifications and standards. The timing was right for such an initiative because with the end of the Cold War defense contractors significantly reduced their workforce and began to concentrate on their core strengths. This consequently led to equally significant increases in the outsourcing of component and subsystem requirements. [10]

1. Advantages of COTS

Unlike in the past, when military requirements were the impetus for experimentation of many new technologies, private market sector forces are now driving technology development in an effort to be first-to-market and ultimately gain market share. With much of the development of new technologies already accomplished, DoD can gain low cost, high performance, and rapid availability from the incorporation of COTS. Flexibility to adopt COTS allows for faster technology insertion and rapid prototyping to meet requirements.

2. Disadvantages of COTS

While it is clear there are significant advantages to using COTS products in defense systems there are also equally important detractors that must also be considered when utilizing COTS. Perhaps the most obvious is that military systems typically operate in harsh environments that many commercial products are not normally designed for. This leads to questions about the reliability and durability of COTS components. The use of products outside their specifications or military alteration of products, such as hardening, will normally invalidate any warranties and terminate contractor support. There may be opportunities to have COTS suppliers modify systems for military use, but often this results in the loss in the economy-of-scale benefit that COTS enjoys. This is due to the fact that DoD lacks sufficient market strength to make it economical for manufacturers to design to military requirements. As an example, "1998 figures indicate that DoD purchased about $500 million in COTS application software, compared with a U.S market of $50.4 billon and an international market of $89 billon." [11] With a market share of less than 1%, DoD is not in a position to influence the design of many COTS products.

Security is also critical concern when using COTS products. Especially when dealing with information systems, widespread commercial use can lead to vulnerabilities being common knowledge. There is no doubt that information is equally as important in the commercial sector and there will always be individuals who want to gain access to proprietary information through whatever means possible. As a result information operations are being conducted each and every day in the private sector, ultimately the techniques used there could be used against similar military systems.

Although at first it may seem counterintuitive, obsolescence must actually be a consideration when employing COTS products. Information systems built upon the latest computing and communications technology may be quickly overcome by continued rapid advancements in these areas. Commercial product life cycles continue to shorten with these rapid innovations, which eventually could lead to the inability to get replacement components for DoD information systems. Ultimately the life cycle of DoD systems must also be shortened to keep up with the commercial sector.

THIS PAGE INTENTIONALLY LEFT BLANK

III. WIRELESS NETWORKS

A. INTRODUCTION

Until relatively recent the term "wireless" was long associated with Guglielmo Marconi's discovery of the wireless telegraph in the late 19th century. The technology explosion of the information age has since changed the connotation of "wireless" for a whole new generation to which it now, more likely infers mobile communications, in the form of either cellular phones and/or wireless computing. Although it may seem hard to fathom for some, it was not too long ago that cellular phones were viewed as an unnecessary luxury and any connection to the Internet was only for a select few individuals in academia or government. As a result of rapid growth in the communications and computing industries one can hardly go a day without hearing advertisements for some form of wireless communications. Cellular telephones are now accepted as a necessity, and although currently not nearly as universal, wireless connection to email and the Internet with personal digital assistants is becoming more commonplace. For certain there are many applications for which the term "wireless" is appropriate, but to keep within the scope of this thesis the remainder of this chapter will address areas pertinent to WLANs.

B. WIRELESS LOCAL AREA NETWORKS

WLANs use electromagnetic waves, radio or infrared, to communicate information from one point to another without relying on physical connections. They provide all the functionality of wired local area networks (LAN), but without the physical constraints of the wire itself. Although some may argue that productivity metrics do not support such a statement, there is little question that the ability to network individual computers has increased efficiency in the world's office environments. The emphasis in the previous statement should be on the words "office environments". This is because the physical requirements of a LAN limited its use principally to stationary applications.

This restraint however is quickly being eliminated with rapid advancements in the WLAN industry. Table 3 lists just some of the major benefits offered by WLANs.

• Mobility	Not restricted to fixed locations
• Installation Speed	No need to pull cable through walls or ceilings
• Cost of Ownership	Lifecycle costs should be significantly reduced
• Scalability	Variety of topologies available to fit needs

Table 3. WLAN Benefits

Without going into detail, one common misconception held by many is that “wireless” and “mobile” are synonymous. Actually they are not; wireless addresses media access sharing issues, while mobile takes into account routing and addressing issues. You can have wireless without mobility, but you cannot realistically have mobility without wireless. Currently limited mobility is available with present protocols, but a great amount of research is being conducted in this area to enable true mobility.

Although wireless computing dates back to the 1970’s, the commercial market, and therefore significant development, did not gain momentum until the 1990’s. Initial wireless systems were proprietary in nature, and although they shared many common physical operating characteristics, there was little interoperability between different manufacturers’ products. Building upon their earlier experience with the advance of wired LANs, industry leaders realized the need for interoperability that can only be achieved through a common standard. Even though significant effort has been put forth to agree on only one common standard there are still several standards competing to gain market acceptance. The most noteworthy standards are listed in Table 4.

Standard	**Data Rate (Mbps)**	**Frequency (GHz)**	**Modulation**	**Physical Layer**
IEEE 802.11	1 / 2	2.4	2 / 4 GFSK DBPSK DQPSK 4 / 16 PPM	FHSS DSSS IR
IEEE 802.11a	6 to 54	5	OFDM	DSSS
IEEE 802.11b	1 / 2 / 5.5 / 11	2.4	CCK	DSSS
HiperLAN/1	1.6	2.4	GFSK	FHSS
Bluetooth	24	5.2	GMSK	Narrowband

Table 4. WLAN Standards

The decision upon which standard to buy into when contracting for large scale WLAN system can be momentous. Should the chosen standard ultimately lose favor and eventually dissolve the ability to get continued support could be greatly jeopardized. Although the Hiperlan standard has gained significant support in Europe and Bluetooth is generating a lot interest throughout the world, for now it appears as if the IEEE 802.11 standard has won the initial battle for market share. As previously mentioned, the ELB WLAN is compliant with the IEEE 802.11 standard and the remaining discussion will be restricted to IEEE 802.11 WLAN systems.

C. IEEE 802.11 STANDARD

From the very beginning during development of the IEEE 802.11 standard the goal was to ensure that WLANs would provide the same functionality as, and be fully interoperable with, IEEE 802 wired LANs. In other words, it must be transparent to the user whether or not the information is traveling via wired or wireless means. To accomplish this task the new WLAN standard would have to support all the protocols and management tools that operate in such wired networks. [12]

Because the IEEE 802.3 standard, or Ethernet, is the most widely accepted LAN it is not surprising that the 802.11 standard is designed with the same interface. And just like the IEEE 802.3 standard, which focuses on the bottom two layers of the Open Source Interconnection (OSI) Model, the 802.11 standard specifies operations below the Logical

Link Control (LLC) Sublayer of the OSI Model Data Link Layer. The 802.11 standard itself defines a medium access control (MAC) sublayer, MAC protocols and services, and three physical (PHY) layers. The three PHY layers are an infrared (IR) baseband PHY, a frequency hopping spread spectrum (FHSS) radio in the 2.4 GHz band, and a direct sequence spread spectrum (DSSS) radio in the 2.4 GHz band. Figure 3 depicts the interface of 802.11 MAC and PHY layers with the LLC sublayer and their relative position within the OSI Model. As originally designed and ratified in 1997, the 802.11 standard specified transmission rates of 1 and 2 Mbps. Almost immediately it was recognized that the low throughput would be a significant liability in the standard gaining widespread acceptance. When compared with an Ethernet transmission rate of up to 100 Mbps, the throughput was simply too low to make it cost effective for businesses to make the investment in wireless. In 1999, the IEEE ratified the IEEE 802.11b "high rate" amendment that added two higher throughput rates of 5.5 and 11 Mbps. DSSS is the only PHY specified in the 802.11b standard. The higher transmission rates are possible due to enhanced modulation techniques not included under the original standard. Additionally, work continues on an IEEE 802.11a amendment that defines operations at 5 GHz with speeds up to 54 Mbps. The ELB WLAN is compliant with the 802.11b amendment of the standard and therefore further discussion will be restricted to it.

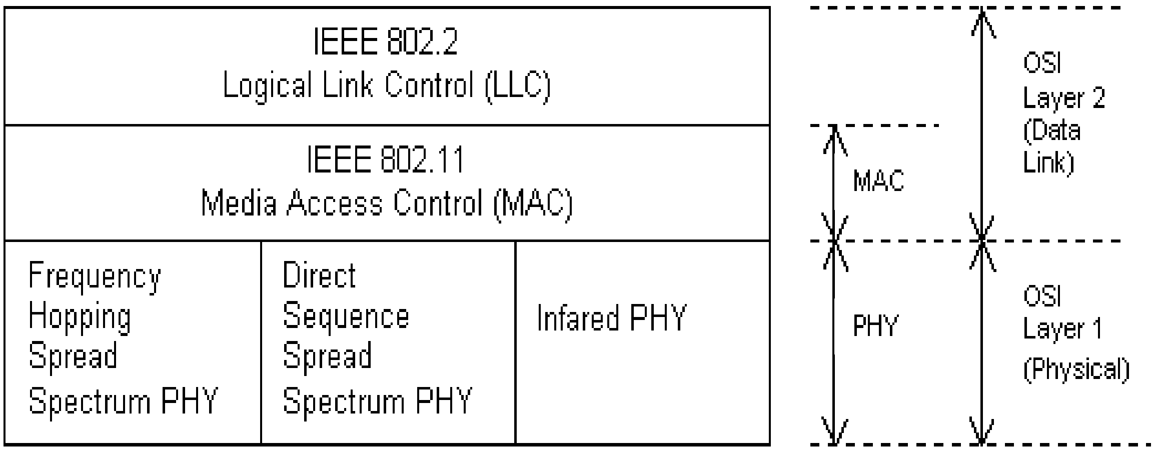
IEEE 802.2
Logical Link Control (LLC)
IEEE 802.11
Media Access Control (MAC)
Frequency Hopping Spread Spectrum PHY
Direct Sequence Spread Spectrum PHY
Infared PHY
MAC
PHY
OSI Layer 2 (Data Link)
OSI Layer 1 (Physical)

Figure 3. IEEE 802.11 standards mapped to OSI reference model [From: 13]

D. NETWORK TOPOLOGY

Physically a WLAN is very easy to establish. Although a WLAN can actually be established with only the individual stations themselves, the typical set up will also include at least one access point (AP). The means of communication between the individual stations and possibly, the wired network, allows for a variety of topologies depending on the individual requirements.

1. Station

The station is the device that connects to the wireless medium; generally it is the network adapter or a network interface card (NIC). It is the component that houses the MAC and PHY layer functionality. The station may be mobile, portable, or stationary. Most often the station will simply be a laptop computer with a WLAN NIC, commonly referred to as a client. An AP is a unique station that is normally in a fixed or stationary location and provides relay or distribution services. APs are very often connected directly to the wired network.

2. Basic Service Set

The basic service set (BSS) is the most fundamental unit of the wireless network. It is simply a set of stations that communicate with one another. There are two types of BSS; an Independent BSS (IBSS) and an Infrastructure BSS.

The IBSS consists of clients that communicate with each other without the use of an AP. Figure 4 illustrates a simple IBSS. Each individual client does not need to be able to communicate with every other client to be active in the IBSS; rather it only needs to communicate with at least one other client. However, since there are no relay services in an IBSS a client can only exchange information with those clients within communication range. IBSS are most commonly referred to as “Ad-hoc networks” that are set up for a specific purpose and are generally short lived.

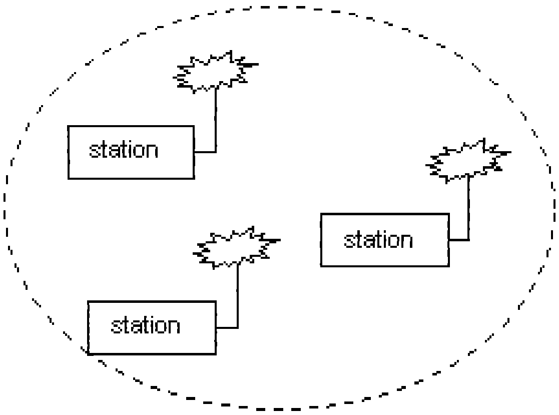

Figure 4. Basic Service Set [From: 13]

An infrastructure BSS (Figure 5) consists of one AP and a number of clients. The AP provides relay services for the BSS and can provide connection to a wired LAN. All clients communicate directly with only the AP, rather than with each other. Therefore a client does not need to be within range of another client in order for the two to exchange information. Instead all communications are first sent to the AP and then from the AP to the destination station. Of course this apparent range gain comes with an associated cost; as a result of the AP relay, communications within the BSS consume twice the bandwidth that they would consume if the individual clients communicated directly with each other.

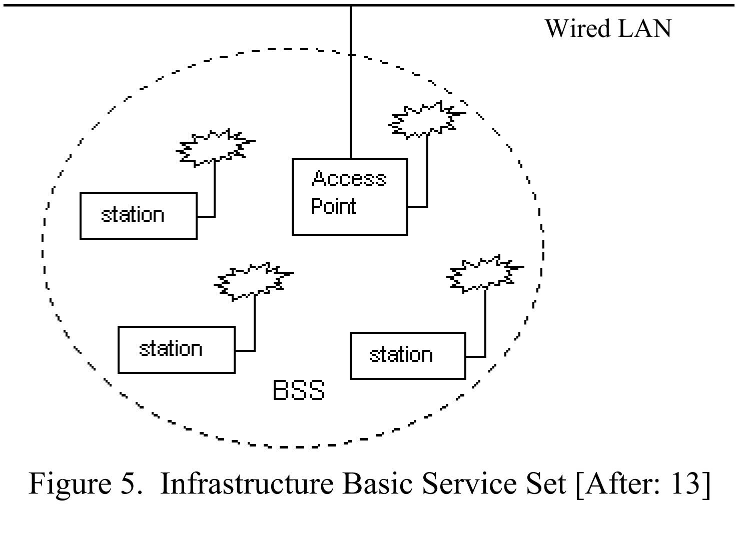

Figure 5. Infrastructure Basic Service Set [After: 13]

3. Extended Service Set

The true benefit of wireless computing cannot be enjoyed if one is restricted to being within range of a fixed AP in order to communicate. The 802.11 standard extends the range of mobility by defining the next logical extension to the BSS; which is referred to as an extended service set (ESS). An ESS consists of two or more infrastructure BSSs where the APs communicate between themselves to forward traffic from one BSS to another. In addition the ESS facilitates the movement of clients amongst BSSs. Figure 6 depicts a typical ESS.

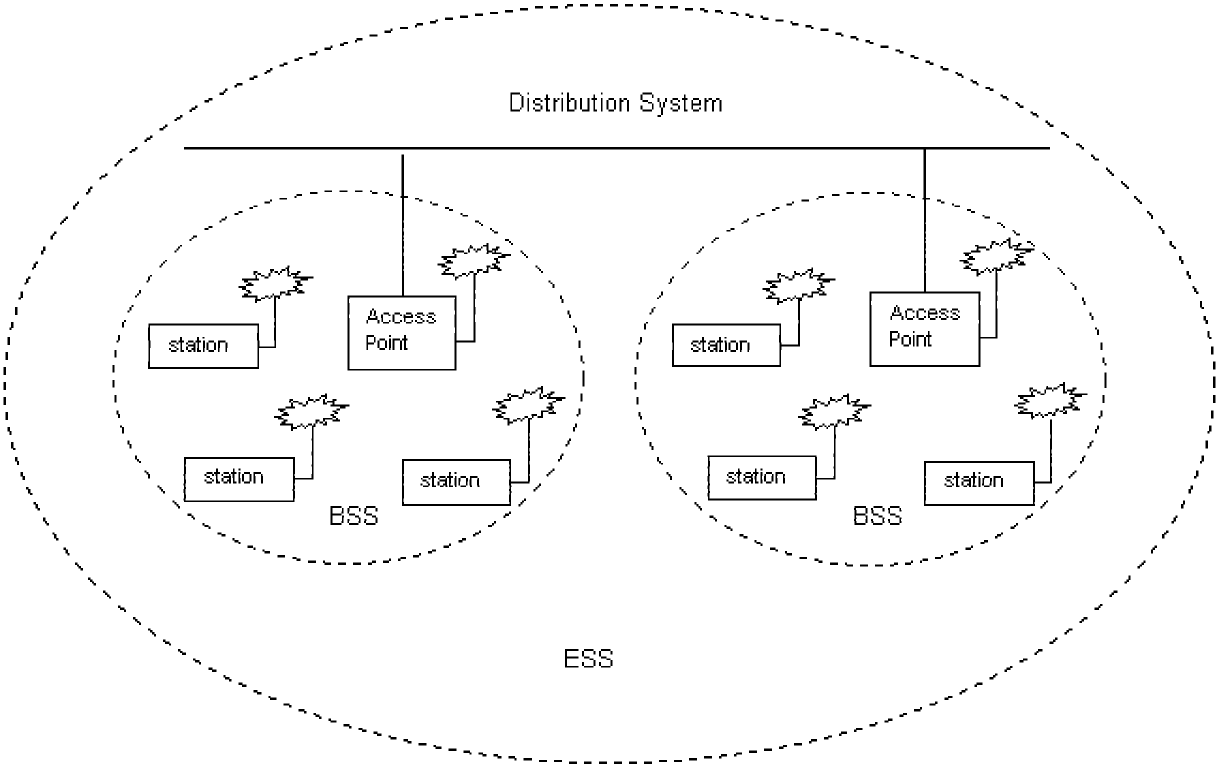

Figure 6. Extended Service Set [From: 13]

a. Distribution System

The APs communicate with each other via the distribution system (DS), which can be either wired or wireless. The DS is therefore the backbone of the WLAN. Each AP receiving information must determine whether the information is to be relayed within the BSS, forwarded along the DS to another AP, or simply to another destination in the wired network outside the ESS. As seen by the network outside the ESS, the ESS and all the mobile clients appear as a single MAC-layer network where all the stations are physically stationary. The 802.11 standard does not place restrictions on how the DS is implemented; only the services it must provide. [12]

E. IEEE 802.11 PHYSICAL LAYER

As previously mentioned, and as illustrated in Figure 3, the 802.11 standard defines three PHYs: DSSS and FHSS in the 2.4 GHz band, as well as an IR PHY. The 802.11b standard to which the ELB WLAN is compliant, however, only defines one PHY, that is DSSS in the 2.4 GHz band. The 2.4 GHz band was chosen because it is one of three frequency bands that make up the almost worldwide-unlicensed Industrial, Scientific, and Medical (ISM) bands. See Figure 7 for an illustration of the frequencies that are covered by the ISM band.

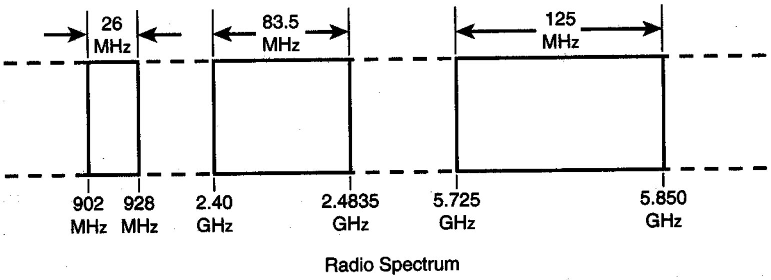

Figure 7. Industrial, Scientific, and Medical Bands [From: 14]

The principal advantage of using one of these bands is that users are not required to obtain a license, as long the power output of their transmitter is less than the levels shown in Figure 8. The 2.4 GHz band offered the best compromise between the advantages and disadvantages of using the higher or lower ISM bands. DSSS was selected as the sole PHY for the higher rate standard because rates higher than 2 Mbps are not possible with FHSS without violating Federal Communications Commission (FCC) regulations. [15]

1000 mW	North America

100 mW	Europe
10 mW/MHz	Japan

Figure 8. Maximum Allowable Transmit Power [From: 12]

As illustrated in Figure 9, the 802.11b standard defines fourteen channels that are centered across the 2.4 GHz band, spaced 5 MHz apart from each other. From Figure 9 one can also see that not all channels are available worldwide. For example, due to FCC restrictions, channels 12 through 14 are not available in North America.

Channel Number	Frequency GHz	North America	Europe	Spain	France	Japan
1	2.412	X	X			
2	2.417	X	X			
3	2.422	X	X			
4	2.427	X	X			
5	2.432	X	X			
6	2.437	X	X			
7	2.442	X	X			
8	2.447	X	X			
9	2.452	X	X			
10	2.457	X	X	X	X	
11	2.462	X	X	X	X	
12	2.467		X		X	
13	2.472		X		X	
14	2.483					X

Figure 9. DSSS Channels [After: 12]

Each individual channel occupies 22 MHz of bandwidth, so this results in significant overlap amongst the channels. Consequently when multiple WLANs are operated within RF range of each other, in order to eliminate potential interference, the channel arrangement should utilize the three channels that do not overlap; channels 1, 6, and 11.

1. Direct Sequence Spread Spectrum

Because of its central significance to 802.11 WLANs a discussion of DSSS technology is appropriate at this point. Spread spectrum techniques were originally developed during World War II by the military seeking a method of communication that was less sensitive to interference or jamming. The technology was so successful it was not declassified by the military until the 1980's, at which time the FCC authorized its use in the three ISM bands. The term spread spectrum is used to describe any technique in which the bandwidth of the transmitted signal is much wider than the bandwidth of the information signal. The increase in bandwidth above the minimum bandwidth can be thought of as applying gain to the desired signal with respect to the undesirable signal, or noise. The processing gain, G_p, can be defined as:

$$G_p = BW_{rf} \div BW_{\inf} \tag{3.1}$$

where BW_{rf} is the bandwidth of the transmitted signal and BW_{inf} is the bandwidth that would be required if only the baseband information was transmitted.

The processing gain is essentially the improvement over conventional communication schemes due to the spreading applied to the signal. The characteristics of spread spectrum signals listed in Table 5 make them attractive for wireless applications.

- Low power spectral density so the signal looks like noise to other radios
- High immunity to jamming and interference
- High resolution ranging
- Possibility for code division multiple access

Table 5. Characteristics of Spread Spectrum Signals [After: 16]

Direct sequence systems are perhaps the best known and most widely used spread spectrum systems. DSSS signals use a spreading code of digital bits, also known as chips, to spread the bandwidth beyond the minimum that would otherwise be required to transmit the information alone. This is accomplished by modulo-2 adding the chips to the information data bit stream with the resulting stream modulating the carrier signal. In order to achieve the same data rate as before the spreading, the resultant data must be sent at a rate equal to the original rate multiplied by the number of spreading bits. And because this means a shorter duration for each unit of digital transmission, and given the inverse relationship between transmission time and bandwidth, the ultimate bandwidth of the combined signal is increased. Remembering that the ultimate objective of the spreading process is to achieve a processing gain that makes the transmitted signal less susceptible to interference, the logical means to accomplish this would be to use a long spreading code. This is often limited by restrictions placed on the allocated bandwidth of the transmitted signal. Recall that, due to FCC restrictions, the 802.11 standard limits the bandwidth of DSSS PHY channels to 22 MHz. The 802.11 standard uses an 11-bit Barker word as the spreading sequence while the 802.11b standard uses a combination of Barker word sequences and an advanced technique known as complimentary code keying (CCK). Figure 10 illustrates an example of DSSS using an 11-bit Barker sequence.

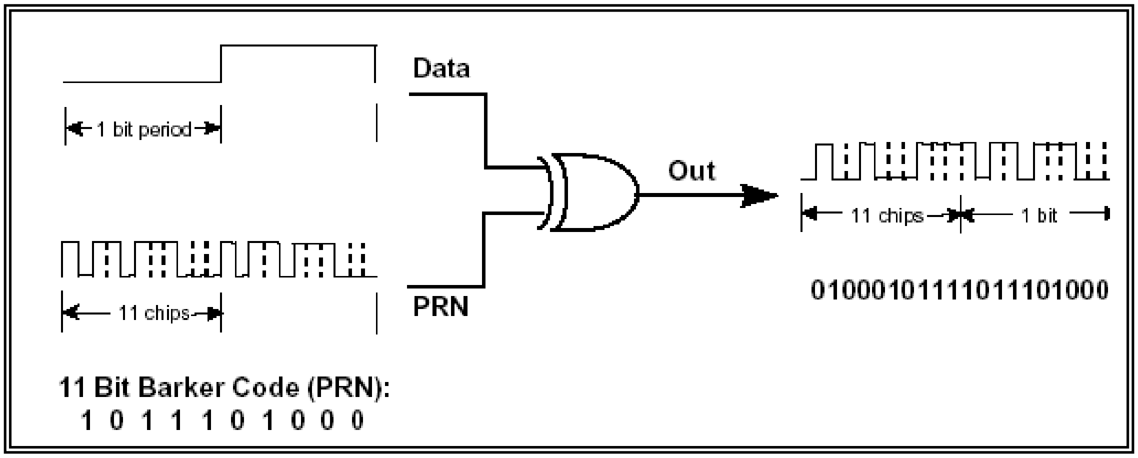

Figure 10. DSSS Modulation with 11-bit Barker sequence [After: 12]

F. IEEE 802.11 MEDIUM ACCESS CONTROL LAYER

The 802.11 MAC contains the protocols required to provide for reliable delivery of user data over a noisy, unreliable wireless media. Although the 802.11 MAC performs some similar functions as the 802.3 MAC, the wireless media that it supports requires some significant modifications to the earlier standard. The three general categories of services provided by the MAC are; reliable data delivery services, fair access to the shared wireless medium, and protection of the data that it delivers. [12] Only some of the most significant MAC services will be address in the following discussion. A detailed discussion of specific frame formats is beyond the scope of this thesis.

1. Basic Access Mechanism

The basic access mechanism employed by 802.11 is carrier sense multiple access with collision avoidance (CSMA/CA). This method is similar to that used in IEEE 802.3 in that it requires a sending station to sense, or listen, prior to transmitting any data. The significant difference between the two is a result of the limitations that many wireless devices cannot receive and transmit simultaneously and that all stations within a BSS may not be within RF range of all the other stations. The latter situation is referred to as the hidden node problem (Figure 11). Therefore rather than relying upon stations to detect collisions, as in 802.3, the 802.11 MAC ensures that collisions are avoided. As depicted, stations 1 and 3 are within range of station 2, but out of range of each other. Prior to station 1 transmitting any data to station 2 it must first send out a ready to send (RTS) packet. The RTS packet tells station 2 the size of the packet that will be sent. Station 2 responds with a clear to send (CTS) packet. Although station 3 cannot receive the RTS from station 1 it can receive the CTS from station 2. As a result it knows not to transmit any data to station 2. All stations receiving either the RTS or CTS set their network allocation vector (NAV) for the given duration. The NAV prevents stations from transmitting over another packet even if it cannot physically sense a transmission in progress. The NAV is therefore a virtual carrier sensing mechanism. [12] Finally after the data packet is received the receiving station sends out an acknowledgement (ACK) packet. Using the above example illustrated in Figure 11, station 3 knows that the medium is clear when it receives the ACK packet from station 2.

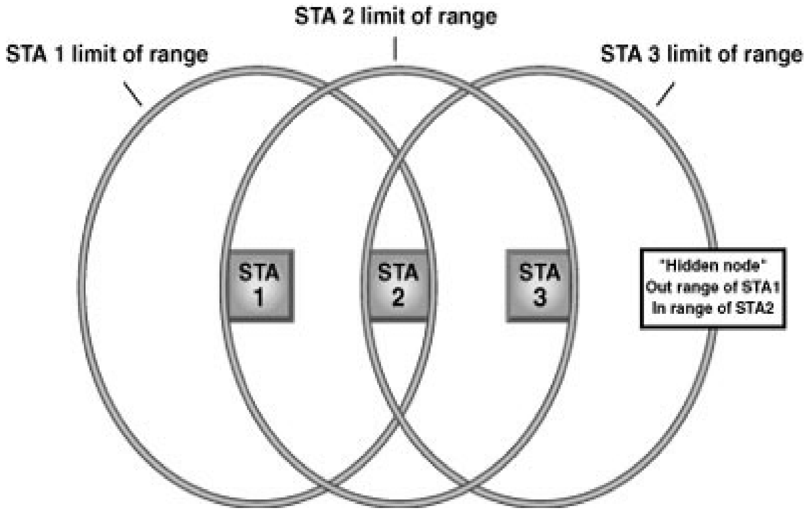

Figure 11. Hidden Node Problem

This example is an illustration of the Distributed Coordination Function (DCF). As the name implies, control of the network is spread between all the participating stations. Essentially it becomes a first-come, first-serve type environment. This may not always be a desirable situation, especially when dealing with time-bounded data.

a. Point Coordination Function (PCF)

As opposed to the mode of operation described above, in the PCF mode a single AP controls access to the medium. The PCF mode uses a poll and response protocol to eliminate any possibility of contention for the medium. While in the PCF mode the AP regularly polls stations for traffic while also delivering traffic to the stations. The PCF is not a stand-alone mode; rather it operates over the DCF. While the AP is in control the network is said to be in a contention-free period (CFP). During this period access to the medium is completely controlled by the AP. The CFP alternates with a contention period where the normal CDF rules operate and all stations can compete for access to the medium. [12]

2. Distribution Services

In an ESS there must to be a means of determining which BSS a station belongs to so that data meant for that station is relayed through the proper AP. In addition there should be some way of verifying whether a station should be allowed to communicate with an AP. These tasks are handled by the distribution services, in association with the authentication and deauthentication services, of the 802.11 WLAN. Although technically a thin layer above the MAC and below the LLC sub layer, the distribution services are most closely associated with the MAC layer and are therefore addressed as such. The five individual services that comprise the general category of distribution services are: association, reassociation, disassociation, distribution, and integration. These services work together within each station to determine two variables that are necessary for communication with an AP. The two variables are the authentication and association states. A station may be authenticated with many different stations simultaneously, but may only be associated with one AP at a time. [12]

The following is a general sequence of how a station transitions between states, but does not cover in detail the specific data exchanged to enable transitions (Figure 12). Each station begins operation in state 1, both authentication and association states are false. While in state 1 a station is authorized limited communication with the AP. The authorized communications are only enough to identify an AP and enable transition to state 2. If a station becomes authenticated it will transition to state 2.

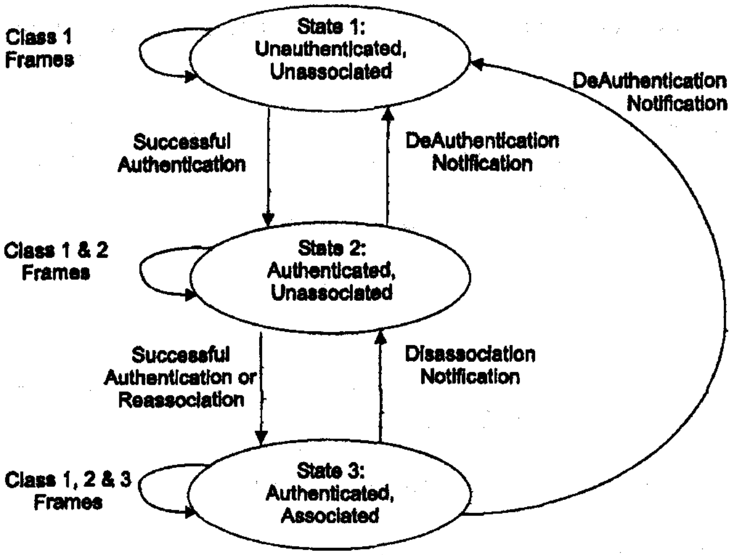
Class 1 Frames
State 1: Unauthenticated, Unassociated
DeAuthentication Notification
Successful Authentication
DeAuthentication Notification
Class 1 & 2 Frames
State 2: Authenticated, Unassociated
Successful Authentication or Reassociation
Disassociation Notification
Class 1, 2 & 3 Frames
State 3: Authenticated, Associated

Figure 12. Relationship between State Variables and Services [From: 12]

While in state 2, a station is permitted additional communications that provide it the capability to initiate the association and reassociation services. A station will remain in state 2 until it is successful in becoming associated with an AP. Once a station becomes associated, and the association state is true, it will transition to state 3.

In state 3 a station is permitted the full range of communications within the BSS. A station will remain in state 3 until it receives either a disassociation or deauthentication notification. If the station receives a disassociation notification it will transition to state 2 and if it receives a deauthentication notification it will transition directly to state 1.

Because a station is permitted authentication with many stations at one time, it follows that it may be in state 2 with more than one station. However, because a station can only be associated with one AP, it may only be in state 3 with a single AP at any one time. As a station roams through an ESS it will transition between states with the various APs that compose the ESS. When a station associates or reassociates with a second AP the original AP that it was associated with receives notification and sends the station a disassociated notification which transitions the station back to state 2 with respect to the original AP. The network knows which AP to relay a station's data through by a BSS Identifier (BSSID) that is part of the address field. As the station roams between BSSs the BSSID changes accordingly. [12]

3. Privacy

Because the wireless medium is significantly different than that of the wired LAN the 802.11 standard defines MAC-level mechanisms to protect data while in transit between stations. Given that there is almost no control over where the RF signal radiates, the WLAN lacks even the minimal privacy provided by the cable in a wired LAN. To compromise a wired LAN the cable has to be physically compromised, a WLAN however only requires an eavesdropper be within range and have an antenna. As a result the standard includes the Wired Equivalent Privacy (WEP) protocol to provide data protection at a level that is believed to be equivalent to that of a wired LAN. [12]

WEP provides encryption of the data frames by passing them through an encryption algorithm. The result is then substituted for the data frame and is transmitted.

A particular point to note is that only the data is encrypted. The header and control information is unencrypted and subject to intercept. As defined in the standard, WEP uses the RC4 encryption algorithm that has a 40-bit key. RC4 is a symmetric stream cipher; meaning the same key is used for both encryption and decryption. The 40-bit key length was agreed upon due to export restrictions placed on 128-bit key encryption algorithms.

Concern regarding privacy has probably been the greatest issue with which the WLAN industry has had to deal with in obtaining widespread acceptance for their products. The free-space in which an RF signal travels seems inherently insecure. Supporters of WLANs point to three features that they assert make their products as secure as a wired LAN. The three features are: spread spectrum transmission, authentication, and WEP. See Figure 13 for an illustration of how these features overlap in the effort to provide security. The spread spectrum technology provides protection down at the physical layer while protection at the data link level is provided by the combination of authentication and WEP.

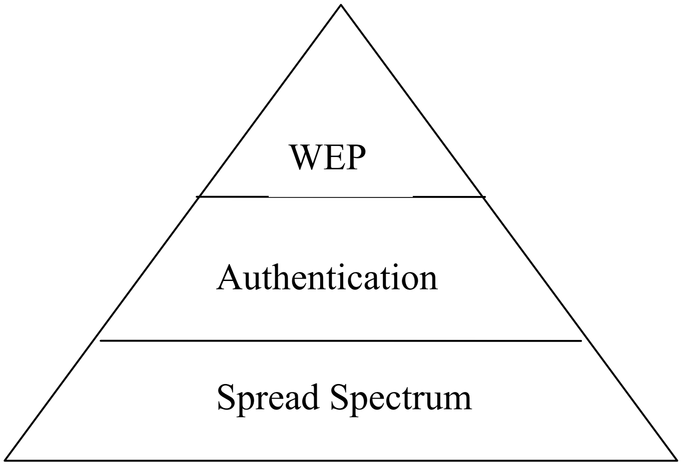

Figure 13. Privacy Pyramid

IV. EXTENDING THE LITTORAL BATTLESPACE ACTD

A. BACKGROUND

The Office of the Deputy Under Secretary of Defense initiated the ELB ACTD in 1997 and USCINCPAC was designated as the program's operational sponsor. The focus of the program, as stated in the Office of Naval Research's program description and guidance for proposals, "…is to exploit the potential of emerging technological capabilities to provide theater-wide situational understanding, effective remote fires and a robust interconnected information infrastructure". [17] As the operational sponsor, USCINCPAC is tasked with providing forces for operational and technological demonstrations and validation of the military utility and sustainability of technology insertions. In order to guide the program, USCINCPAC identified five Critical Operational Issues (COIs) that should be addressed at the conclusion of the ACTD. See Table 6 for a list of the COIs. The program was divided into a number of experiments leading up to two major system demonstrations (MSD) in 1999 and 2001. MSD-1 was conducted in concert with exercise URBAN WARRIOR in June 1999 and MSD-2 was conducted in concert with exercise KERNAL BLITZ-01 in June 2001.

1. Can ELB technologies greatly expand the JTF's capabilities to conduct over-the-horizon collaborative planning and coordination that integrates all necessary elements into a seamless environment (network) to adequately support planning?

2. Can a deployed commander, through enhanced situational understanding and unprecedented battlespace dominance, exercise C2 over disaggregated forces to shape and control the littoral area in ways not possible today?

3. Can an embarked, dispersed task force staff provide sufficient real-time information to dramatically increase force effectiveness while reducing force vulnerability?

4. Can an afloat JTF provide sufficient massed fires support to early entry forces to fulfill the requirements of over-the-horizon call for fire?

5. Can early entry expeditionary forces, through application of advanced technology and concepts, rapidly prepare the battlefield for more movement of C2 ashore and transition to follow-on forces?

Table 6. USCINCPAC Critical Operational Issues [After: 3]

B. ELB ACTD OBJECTIVES

The principal objective of the ELB ACTD is to demonstrate the viability of the revolutionary concept for expeditionary warfare as envisioned in OMFTS and to integrate advanced technologies that will enable such a significant doctrinal shift. The goal is to integrate the command element and its dispersed combat units with multiple weapons systems and sensors in a manner that will defeat a potential adversary in an extended littoral battlespace. Just like OMFTS, the operational concepts of the ACTD place emphasis on intelligence, deception, and flexibility; using the sea as maneuver space; and establishing overwhelming tempo. This concept defuses the traditional concepts involving lines of departure, passage of command, and up and over communications. Rather it requires a seamless command structure between afloat and ashore units with a shared SA and understanding. The commander must have total visibility of his forces; and those forces should be able to call in supporting fire from weapon platforms at sea, or on the ground, or in the air to engage targets at greater distances than ever before possible. But this new concept does not stop at the commander level; for OMFTS to be successful the communications infrastructure and fires-and-targeting capability must support the smallest combat unit. This will enable a more flattened informational structure that should result in an increased flow of information. In the end this should lead to the greater optimization of resources that is critical to OMFTS. [17]

The advanced technologies linked with this ACTD are divided into four core functional areas: remote sensing and intelligence, communications and networking, C2, and fires and targeting.

1. Communications and Networking

The communications and networking objective is to provide a wireless, wide-area relay network (WARNET) to support expeditionary forces operating within a Joint Task Force (JTF) framework. The WARNET should provide the backbone communications critical to the C2, intelligence, and reconnaissance functions. It should give an over-the-horizon capability that is organically controlled.

2. Command and Control

Within the C2 area the program objective is to make available shared combat information orders to support expeditionary forces operating within a JTF framework. Shared combat information is necessary to support an accurate and timely common tactical picture (CTP), as well as aid in the preparation and dissemination of plans.

3. Fires and Targeting

The objective within the fires and targeting technology area is to provide the means to exploit fires from sea, air, and land by coordinating, assigning, and directing weapons systems on targets. Enhance lethality should be achieved through improved response times and massing fires, while simultaneously reducing the potential for fratricide.

4. Sensors and Intelligence

The direction for the sensors and intelligence technology area is to integrate selected sensor systems into the CTP, thereby aiding in the dissemination of intelligence within the operations area at the tactical level. Imagery should always be available to those who need it. Contacts and reports from organic sensors must be automatically distributed to operating forces.

The remainder of this chapter will focus on the communications aspect of this ACTD. As this is where the WLAN, that is the focus of this thesis, fits into the program.

C. ELB COMMUNICATIONS

After reviewing the above core technology areas it is clear that there is extensive overlap, or interdependence, amongst the various functional areas. No one area of technology can provide significant benefit without one or more of the others. However, it is also apparent that an effective communications network is central to successful achievement of the overall objectives. Without reliable communications there is no CTP, nor a means to disseminate plans, or a method to call for fire or provide imagery to those who need it. The WARNET has received considerable attention due to this reliance on an effective communications system. The requirement to support the forward deployed, mobile Marine is what initially led the network designers to look towards a wireless solution. The Navy and Marine Corps have many fixed land-based networks that can provide the required services, and with enough time they could deploy the infrastructure necessary to establish such a network, but the lead-time and fixed infrastructure is contrary to OMFTS. A list of desired qualities of the envisioned wireless network was agreed upon early in the program and is included as Table 7. At the conclusion of the selection process, which included a six-month competitive design process, General Dynamic’s proposal, which was based on Lucent’s WaveLAN products, was awarded the contract.

- Ability to support point-to-point, multicast, and broadcast packet-switched communications among large and small capacity users over distances up to 300 miles.
- Ability to support point-to-point and group voice service across the entire extended battlespace.
- Ability to include service to Marines and dismounted soldiers with battery-powered radio and computers at rates of at least 64 kbps.
- Ability to include service to large users (ships, mobile combat centers) at rates up to 1.5 Mbps.

Table 7. Desired Qualities of ELB WLAN [From: 3]

1. Communications Architecture

ELB's communications architecture has undergone some substantial revisions during the life of the program. A network that was originally envisioned to be a homogeneous COTS-based, 802.11 compliant WLAN has evolved into a three-tiered network that employs a "system of systems" of COTS technology to provide data and voice communications between individuals, units, and command centers within the littoral battlespace. The WARNET is composed of afloat shipboard nodes, airborne relay nodes, ashore mobile nodes, and End User Terminals (EUTs). Figure 14 provides a high-level depiction of the WARNET.

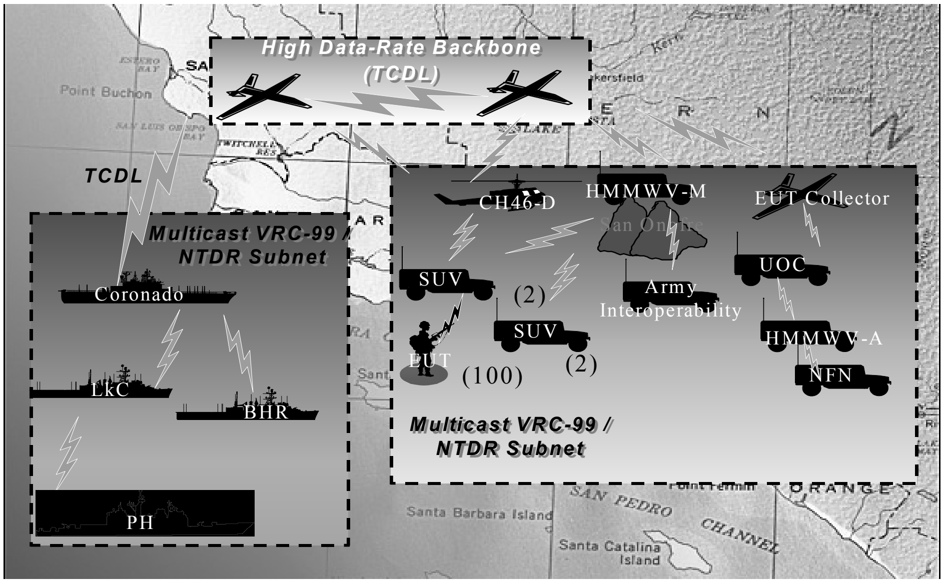

Figure 14. ELB MSD-2 Architecture [After: 18]

Tier 1 connects small dismounted units and vehicles on the ground. Tier 2 links unit headquarters ashore and afloat, and tier 3 provides the airborne communications network that enables over-the-horizon connectivity throughout the battlespace. With the exception of the EUTs, all platforms contain systems from at least two tiers of the WARNET. This is what enables the communications to move between the various tiers. The stations at the higher tiers retain the capability to communicate using lower tier systems. For example, airborne stations that contain tier 3 systems also have the ability to communicate with EUTs through onboard APs. This allows EUTs that may be out of range of communications vehicles to potentially remain active in the WARNET. The additions to the WARNET were added as a means to mitigate risks associated with operating an 802.11 WLAN at extended ranges. [17] Although the network is significantly different than the initial vision, it still retains the core 802.11 compliant technologies down at the small unit level that is the focal point for the success of OMFTS. A description of major WARNET components, with emphasis on the tier 1 systems, follows.

a. Tier 1

Tier 1 composes the 802.11b compliant WLAN portion of the WARNET. The two primary components of the WLAN are both Agere Systems products, ORiNOCO Gold PC Cards and ORiNOCO AP-1000 Access Points. (Note: Agere Systems is a subsidiary of Lucent Technologies and the previous Lucent WaveLAN family of products now is sold under the ORiNOCO name.)

The ORiNOCO Gold PC Card is a PCMCIA card that is used in conjunction with a Panasonic Toughbook notebook computer to form a EUT that in turn provides network access to the individual unit in the field via an AP. In order to remain consistent with OMFTS, the principal physical limitation for the EUTs are that they be man-portable and be sufficiently light as to not hinder rapid movement within the littoral battlespace. This requirement places a constraint on the size and number of batteries that can be used, and hence battery conservation is a critical design consideration. See Figure 15 for an illustration of a EUT. Being 802.11b compliant, the Gold PC Card supports data rates up to 11 Mbps.

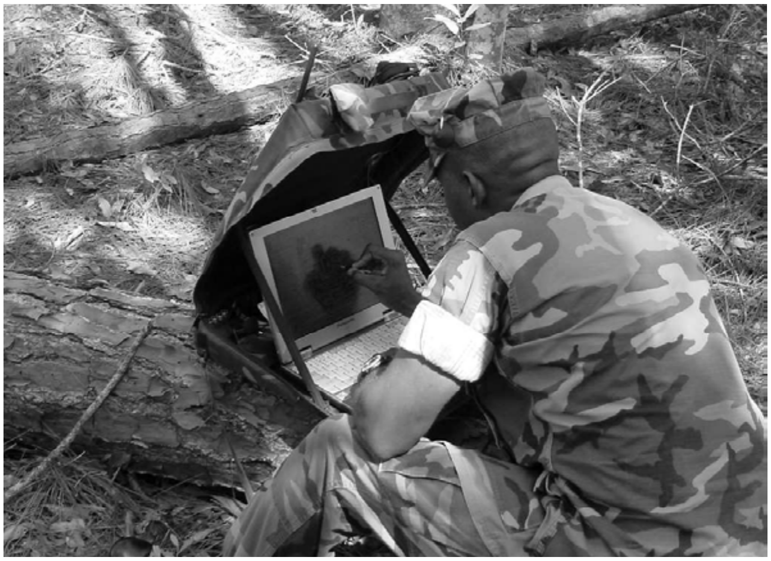

Figure 15. End User Terminal [After: 18]

Within the WARNET, the ORiNOCO AP-1000 Access Points provide the interface between tier 1 WLAN subnets and also provide the interface between tiers 1 and

2 systems. As discussed in Chapter III, an AP can either provide direct connectivity between a wired network and a wireless unit, or it can be used to interconnect multiple APs. For the ELB network the APs serve in both roles, but rather than connecting the WLAN to a wired network they connect it to another form of radio network; which forms tier 2 of the WARNET. Communications vehicles and airborne relays serve as the platforms that provide the primary access to the WARNET for the individual field units. While during MSD-2 specially configured sports utility vehicles acted as communications vehicles during an actual operation this role would be performed by high mobility multipurpose-wheeled vehicles (HMMWV). Similarly, during actual operations the intent is to have unmanned aerial vehicles (UAV) serve as the airborne relay, during MSD-2 this role was performed by commercial Crownair aircraft and a CH-46D helicopter. Figure 16 is a schematic illustration of the architecture for a typical AP in the WARNET.

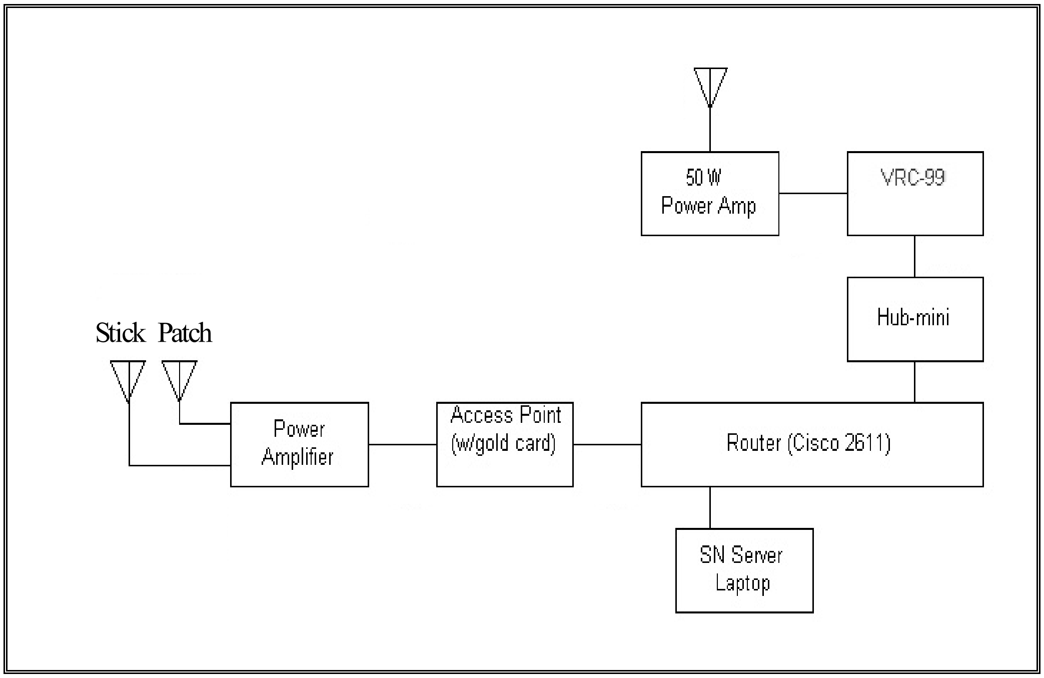

Figure 16. Communications Vehicle Schematic [After: 18]

Given that the ORiNOCO products are 802.11b compliant the operating characteristics of the WARNET WLAN are in many respects very similar to that described in Chapter III. The WLAN operates in the infrastructure mode, whereby all communications are relayed through an AP prior to reaching its destination. Each tier 1 subnet serves as a BSS while the entire range of tier 1 subnets form the ESS. The RTS/CTS protocol is utilized as a means to avoid collisions. The system employs the improved WEP protocol, RC4 128-bit encryption. It should be noted that because this is commercial grade encryption, as opposed to National Security Agency (NSA) Type-I grade encryption, the WLAN portion of the WARNET is limited to Sensitive But Unclassified (SBU) data.

As one would expect, however, due to the unique environment in which the WLAN is expected to operate there are some significant modifications that were made to the off-the-shelf ORiNOCO products. Normally operating in the ISM 2.4 GHz band, the transmit frequency is modified by a power amplifier to avoid interference with commercial products. The ORiNOCO products normal transmit power is 32 mW, which is well within the 1-watt FCC restriction for the ISM band, as depicted in Figure 8 in Chapter III. Because the ranges associated with the littoral battlespace are vastly greater than the office environment for which the products were originally designed the EUTs and APs transmitter power output had to be increased. This also was accomplished by the power amplifier, where the EUT transmit power was increased to 6 watts while the APs were amplified to 30 watts. Although some extended ranges were recorded during field tests, especially between the 30-watt AP transmitters, the average range from EUT to airborne relay was 20 km.

b. Tier 2

The core components of WARNET tier 2 are the AN/VRC-99A radio and the Near Term Digital Radio (NTDR). Both radios provide sufficient range, as well as adequate data transmission rates, for operations on an extended battlespace. In addition, they each incorporate DSSS modulation, as well as communication security (COMSEC) algorithms that are designated NSA type 1; hence they are cleared for the transmission of classified data. Although they are self-configuring, and therefore capable of mobile communications on a wheeled platform, their physical size restricts their use from dismounted troops. Because they are capable of greater range than the APs, these radios are capable of transmitting data between two tier 1 subnets that are geographically separated, as well as serving as a relay between the tier 1 and 3 systems. Together with the tier 3 systems, the VRC-99A and NTDR form the backbone of the WARNET.

c. Tier 3

The Tactical Common Data Link (TCDL) comprises the WARNET's third tier; the long-range backbone of the network. This system provides reliable point-to-point data link that facilitates line-of-sight (LOS) communications over long distances. It was originally designed for connectivity between UAVs and ground stations with a 10.7 Mbps data rate at 150 nm. Within the WARNET the TCDL provides the backbone connectivity between the command ships afloat and the airborne relay stations. The TCDL was present onboard the USS Coronado, as well as the airborne stations during MSD-2. Figure 17 is a schematic of the tier 3 architecture onboard one of the airborne stations.

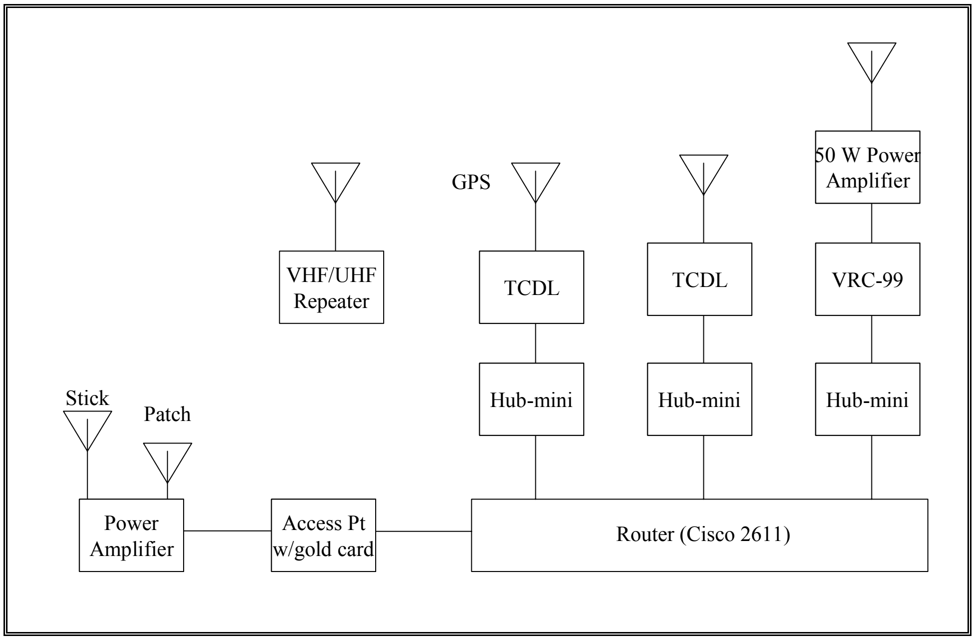

Figure 17. Tier 3 Architecture [After: 18]

V. POTENTIAL VULNERABILITIES

A. INTRODUCTION

By identifying information superiority as the foundation upon which future operational concepts are to be based, JV 2010 in essence acknowledged that communication systems would have a greater influence on the future success of U.S. forces than at any time in the past. The shift from information superiority to communication systems is not meant to imply that they are synonymous, for they certainly are not. Communication systems merely exchange data, while information systems attempt to transform data into information with the intent of increasing the knowledge base and aid decision-making. However, it is because information systems rely upon an exchange of data that allows one to anticipate the critical role that communication systems will play in future conflicts. By understanding the requirement to achieve information superiority, it can be assumed that all forces in future conflicts will channel a great deal of effort towards employing the most capable and reliable communication systems. But this is only half of the information superiority problem set, for history illustrates that forces will expend almost an equal amount of effort attempting to disrupt or deny the enemy's communications.

1. Information Warfare and Vulnerability

Although the concept of IW is not novel, it is the new doctrinal concepts' reliance upon quantities and quality of information never before possible, which has propelled IW to the forefront of tactical thought. While precise definitions may vary, the Air Force's publication "Cornerstones of Information Warfare" defines IW as; "…any action to deny, exploit, corrupt, or destroy the enemy's information and its functions; protecting ourselves against those actions; and exploiting our own military information functions." [19] Within the context of this thesis it is the second part of this definition, "protecting ourselves against those actions", that has the most significance. It is not sufficient to have the most capable communication systems if one does not put sufficient emphasis on robust systems that can defend against IW efforts. The WARNET is just one example of a new communication system that is being proposed with the expectation that it will be able to provide one link necessary towards achieving information superiority and enable operational concepts such as OMFTS. In order to adequately evaluate whether such a system will meet requirements we must assume the role of a potential adversary and look at possible vulnerabilities that may be employed in an IW scenario.

Surely no communication system is totally without vulnerabilities, so a realistic understanding of what a system's vulnerabilities are is necessary to provide decision makers with the background necessary to conduct thorough risk analysis. The mere presence of a system vulnerability is not necessarily a setback if it can be determined that a potential adversary does not possess the capabilities necessary to exploit the vulnerability. To what degree of certainty and for how long the determination will remain valid are the wildcards in the process. There is little question that as a result of the information revolution the world's economy is dependent upon information and communication systems. Given this fact it is also clear that there are individuals who have chosen to exploit vulnerabilities in these systems for financial and personal gain; so as a result IW is no longer limited only to the military sector. This new reality, combined with the military's increased utilization of COTS communication systems, further complicates any risk analysis. For a system that is widely used in the commercial sector has a much greater potential to be exposed to persons seeking to find and exploit vulnerabilities than one used exclusively in the military sector.

a. ELB Communications

The 802.11 standard of WLANs, that comprises tier 1 of the WARNET, is a good example of a standard that has gained widespread acceptance in the commercial sector while at the same time garnering interest for potential military applications. And along with its increasing use in the commercial sector there has been a considerable amount of research into potential vulnerabilities. As one would expect this research has been largely limited to commercial applications of the system. The fact that there is little one can do to geographically restrict data transmission in the wireless medium has caused many to instinctively question the security of such systems. Of course the standards committee and system vendors anticipated many of these initial concerns and have responded by citing the security features in the PHY and MAC layers of the standard that were noted in Chapter III.

In attempting to identify potential vulnerabilities in the ELB WLAN the assumption was that the system would be employed in a tactical environment against an adversary possessing at least moderate technological means that has some knowledge of the presence of a foreign force on its soil. The lack of complete surprise would be reasonable to expect in an OMFTS-type scenario given the presence of surface naval units in the littoral supporting a landing force on the ground. Figure 18 is a depiction of a tactical IW sequence of events and options that an adversary may be expected to employ, and therefore were used to guide the search for potential vulnerabilities in the ELB WLAN.

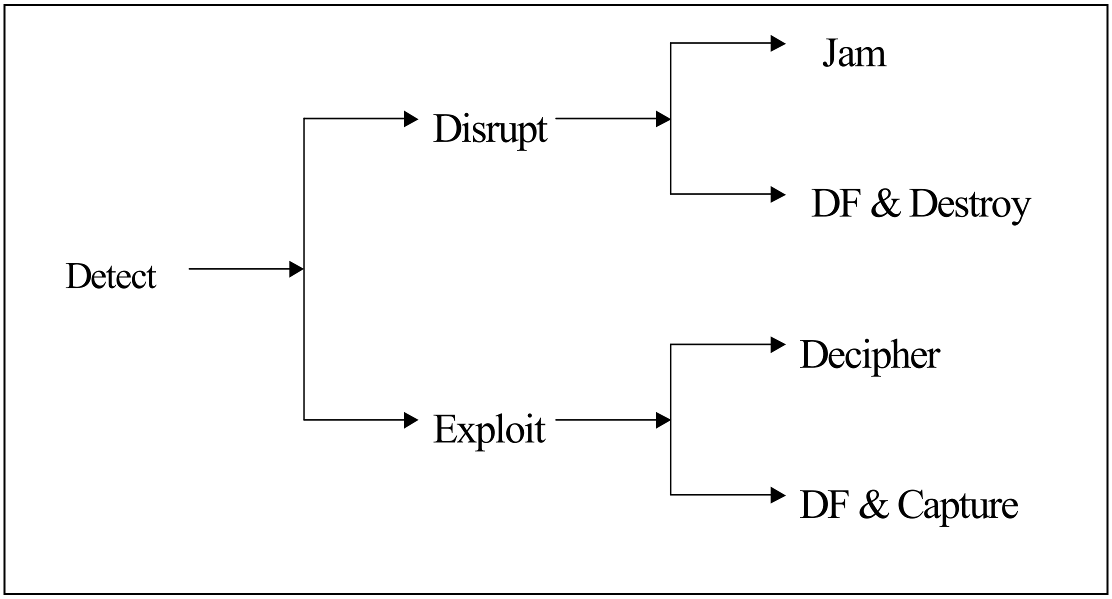

Figure 18. IW Scenario [After: 20]

Any force utilizing an active sensor, such as radar, or a communication system is immediately vulnerable to detection by the enemy once the first RF transmission is made. By its very nature the ELB WLAN is an active system that relies upon a two-way exchange of data between EUTs and APs to remain functional. Should an adversary detect the presence of an RF transmission, depending on the tactical situation and its technological capabilities, it then has the option of either trying to disrupt the transmission or attempt to exploit the transmission in hopes of gaining additional intelligence. Should the decision to disrupt the communications be made the enemy would next have to decide whether to jam the transmission or locate and destroy the transmitter. Should they attempt to exploit the transmission they could potentially gain intelligence by deciphering any encrypted traffic or rather merely maintain contact with the transmitter to monitor friendly force movements. The remainder of this chapter will be a discussion of how the ELB WLAN may be vulnerable to the above IW scenario.

B. DETECTION

If an adversary is unable to detect the RF transmissions of the ELB WLAN then the remainder of the IW scenario does not occur. From the design perspective, vulnerability to detection would appear to be a PHY layer issue. Recalling from Chapter III, the pyramid of privacy features, spread spectrum modulation is the only feature located at the PHY layer; and therefore is the primary means to limit the probability of detection. The following statement is a typical expression by WLAN vendors insinuating the security provided by utilizing spread spectrum modulation in the PHY layer of their systems.

> Originally developed by the military for secure communications, spread spectrum signals are designed to provide negligible interference to the communication of other existing users and indeed, it is difficult to determine if a spread spectrum signal is actually present. We call characteristics of this type Low Probability of Intercept (LPI) and Low Probability of Detection (LPD); they are requirements for successful military communications. [21]

Although the average commercial business that operates a WLAN is not too concerned with having someone merely detect their use of a wireless network, they are concerned about network performance that may be degraded by unintentional interference and security issues such as denial of service attacks and signal intercept.

These issues will be addressed in a following section, because this illustrates the central importance that spread spectrum modulation supposedly plays in the security of WLANs.

1. LPD/LPI

As the previous quotation illustrates, LPD and LPI are often mentioned simultaneously when referring to secure military systems; most often there is no further differentiation between the two terms. LPD refers to hidden signals that make detection by unintended receivers difficult. LPI signals deny the unintended receiver from being able to distinguish their characteristics that could lead to further exploitation. Because the features of LPD and LPI signals are, for all practical purposes identical, they will both be treated as such throughout this discussion. LPD is strictly a matter of signal design, where the goal is to produce uncertainty at the intercept receiver that results in a Signal-to-Noise Ratio (SNR) much lower than would otherwise occur in the absence of such a design. As addressed in Chapter III, DSSS utilizes a spreading code to distribute the transmitted power over a bandwidth much larger than the baseband bandwidth, thereby reducing the power density of the signal, which ultimately makes it harder for an interceptor to detect. Figure 19 illustrates the effect of DSSS spreading; notice in the signal on the left how the transmitted signal is nearly indistinguishable above the noise.

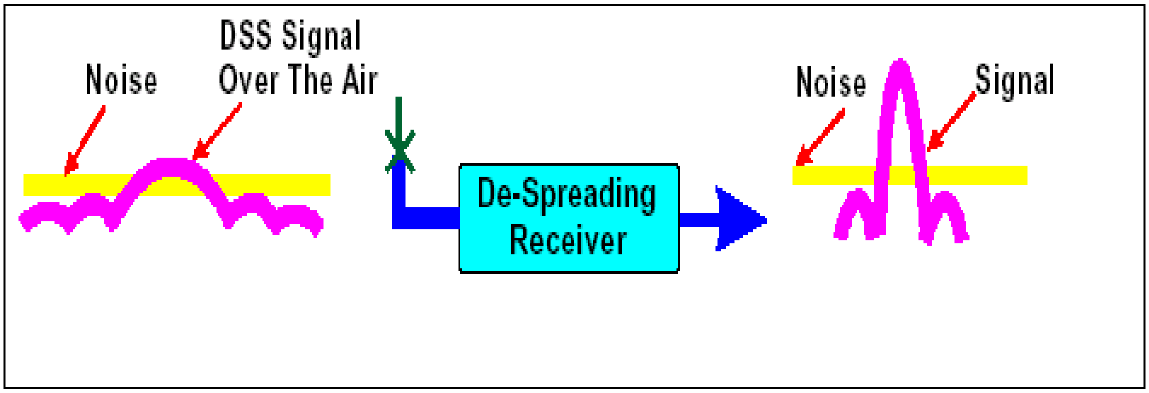

Figure 19. Low Power Density

Given that spread spectrum LPD is directly related to spreading and power it stands to reason that two characteristics of LPD DSSS modulation are large bandwidth and low power output.

a. IEEE 802.11b

To date there has not been any significant public research into the issue of probability of detection for 802.11b WLANS. This is most likely because the standard is so specific in regards to frequency/channel assignment that mere detection of a WLAN signal, given an interceptor is at or inside the range of an intended receiver, is a trivial matter. Within the past year there have been several reports that discussed the ease of detecting companies' WLAN signals while passing by outside their premises. For the ELB WLAN signal detection is not so easy for the reason that, as mentioned in Chapter IV, the RF signal is not modulated to a carrier frequency in accordance with the standard. This modification serves two purposes, first and foremost it complicates signal detection by an unintended receiver, and secondly it removes the signal from the interference and restrictions that are associated with transmitting in the ISM band, which is especially beneficial during CONUS-based exercises.

Just as it is not good enough to accept the mere presence of any firewall as evidence that a network is secure, it would be foolish to believe the utilization of DSSS modulation guarantees LPD. Although it is true that DSSS can provide LPD, much depends on the design or complexity of the transmitter, which of course directly translates into cost. As with just about any communication system there are significant tradeoffs that must be made between security and throughput. The most significant point to remember regarding the 802.11b standard is that it was designed by and for the commercial sector. And although security was a consideration, the standard was driven by the desire to operate the systems, free of any licensing requirements, with minimum interference within the ISM band. The FCC has specific restrictions on transmit power and processing gain upon communications within the ISM band. These restrictions guided the development of the standard. And so this was the genesis of the utilization of spread spectrum technology in the WLAN industry. Subsequently although DSSS transmitters can be designed to transmit LPD signals, this was not the reason for its incorporation in the 802.11b standard; rather it was incorporated principally in order to enable WLANS to operate in the ISM band. And because of this fact, the DSSS signal as transmitted in WLANs does not display the characteristics that one would expect for true military LPD system.

Recall that the two major characteristics of an LPD system are large bandwidth and minimum transmit power. When combined, these two contribute to produce a reduced spectral power density. Keep in mind, however, that the standard was not designed to produce an LPD signal, but rather to conform to FCC restrictions while maximizing performance by minimizing the probability of bit error, P_b. The probability of bit error, or bit error rate (BER), is a function of the signal energy per bit (E_b) to noise density (N_o) ratio (E_b/N_o), where:

$$E_b = P_t / f_b \qquad (5.1)$$

$$N_o = N / BW \qquad (5.2)$$

P_t is the modulating signal power, f_b is the bit rate, N is noise power, and BW is the signal bandwidth.

Figure 20 illustrates the inverse relationship between BER and E_b/N_o; for each form of modulation shown, as E_b/N_o increases BER decreases.

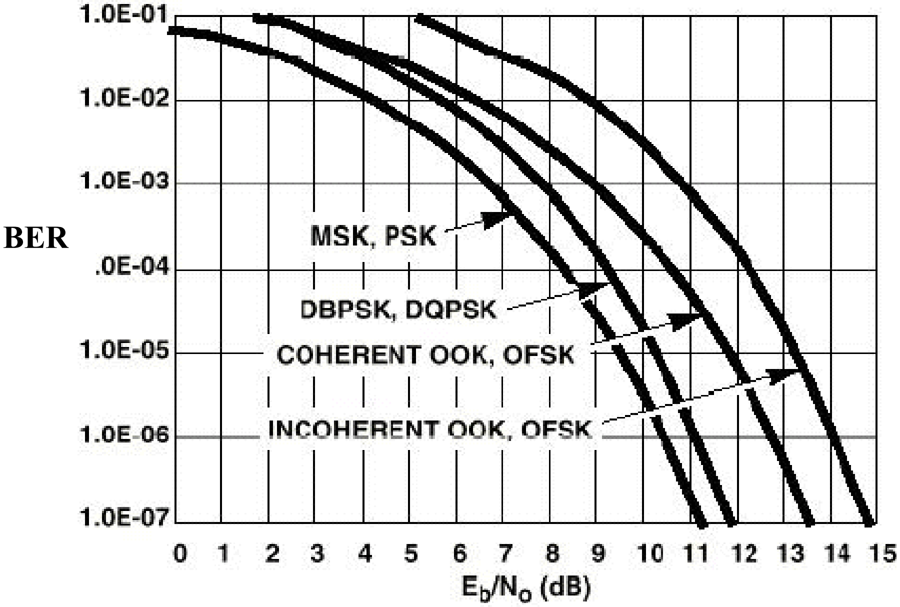

Figure 20. *Eb/No* vs. BER

Notice from Equations 5.1 and 5.2 that the quickest way to decrease the BER without directly impacting throughput is to increase the signal power, *Pt.* This action however is counterproductive when discussing LPD signals, where the design goal is to minimize the spectral power density. The average spectral power density is approximated by:

$$S(f) \cong E_b / K \qquad (5.3)$$

where *K* is the number of chips per bit used in the spreading sequence.

From Equation 5.3 one realizes the critical nature of the DSSS spreading code in LPD transmissions. While most military LPD communication systems utilize spreading code lengths on the order of hundreds or thousands of bits, such as maximal sequences, the 802.11b standard uses either an 11-bit Barker code or 8-bit CCK code. The Barker code was initially chosen for the standard due to its excellent autocorrelation properties that make it ideal in a multi-path environment. The short length of the code reduces the amount of overhead associated with spreading the baseband, therefore enabling greater data throughput. The CCK code was later adopted to enable the higher data rates of the 802.11b standard.

b. ELB WLAN

One system modification that was made to the WLAN for the WARNET actually significantly increases the spectral power density from the commercial standard. Recall from Chapter IV, that through the use of external power amplifiers the peak power is increased from a maximum of 1-watt to 6-watts for the EUTs and 30-watts for the APs. While it is clear that this is done with the intent of increasing the transmission range and decreasing bit errors, it is a good illustration of the tradeoffs or compromises that must be made between performance and security. Given the fact that the APs transmit at a power level five times that of the EUTs it stands to reason that an adversary is on average more likely to detect an AP prior to detecting the EUT. This could be a crucial issue that will be addressed further during the discussion of jamming.

Given the assumption that ELB WLAN is not being employed as part of a covert operation, the mere detection of the signal is not as militarily significant as is the ability to employ direction-finding (DF) techniques to locate the position of the transmitter. The operating characteristics of the WLAN that requires a two-way exchange of management and data frames results in a sufficient number of transmissions that should enable an adversary to DF the signal. This is a particularly true in the case of the AP, which as the central hub of the WLAN, is involved in every exchange of data.

C. JAMMING

Jamming, or denial of service (DOS) attack, is one physical layer security issue that has received some interest for commercial sector WLANS. It stands to reason that when there is the possibility for a significant amount of financial gain by denying someone else the use of their network, there will be individuals or groups who will attempt to exploit the opportunity regardless of the ethical issues involved. Of course financial incentives are not the only motivators for attempting to deny an organization the use of its network. There was a report in April 2001 of a group of Pakistani militants who, while conducting an armed raid into Kashmir, India, were able to delay the Indian response by successfully jamming the wireless network of the local police for two hours. [23] For the purposes of this thesis, jamming and DOS attacks are distinguished as follows; jamming is the intentional insertion of RF energy in the radio spectrum in order to deny the intended receiver access to a transmitted signal, while a DOS attack works above the PHY layer to deny the use of meaningful network services. An example of a DOS attack would be the constant transmission of an RTS signal by an intruder on the network, thereby not allowing any other station from accessing the medium. In fact it is this type of DOS attack that has received a large amount of public interest. Although this could be a valid concern for the ELB WLAN, the more likely scenario in the tactical environment involves the more traditional EW concept of RF jamming.

Just as in the LPD scenario, depending on the complexity of the system, jamming a DSSS system can be a very complicated undertaking. There is one very fundamental difference between the two however, whereas in the detection scenario the adversary's target was the transmitted signal, in the jamming scenario the adversary attempts to target the receiver. Because the receiver is almost always matched to the transmitted signal some of the critical characteristics of LPD systems hold true for anti-jam (AJ) design; most importantly for a DSSS system it is the ability to operate over a large bandwidth. By calculating the AJ Margin one can determine the degree of jamming a system can withstand. The AJ Margin is defined as the maximum factor by which the power of a jammer can exceed the communications signal power and yet the baseband SNR still equals the minimum required value for reliable communications. [22] Put from the jammer's perspective, in order to successfully jam a system with an AJ Margin of 10 dB he would have to introduce a minimum of 10dB of jamming noise. AJ Margin can be calculated as follows:

$$AJM = PG - SNR_o - RL \qquad (5.4)$$

where *PG* is the processing gain, *SNR* is the minimum output signal to noise for reliable communications, and *RL* is system loss in the receiver. Equation 3.1 can be used to determine processing gain. Receiver system loss is a function of the internal system design and for all practical purposes is a constant. The minimum output SNR is dependent on a number of different variables; in general however, it will be greater for the higher transmission rate signals.

The various techniques and strategies for communications jamming is a complex topic that is beyond the scope of this thesis. However, one fundamental issue of wideband versus narrowband jamming of a DSSS receiver is important to address. As opposed to in the transmitter, the spreading code in the receiver actually de-spreads the incoming signal by the same modulo-two addition process to strip away the coding bits and reveal the baseband information that is then passed through narrowband filters; this however is only true for signals that are coded with the same spread sequence that is used in the receiver. Other incoming signals, or noise, are spread across the operating bandwidth therefore reducing the amount of noise actually passing through the narrow band filters. By understanding this process it becomes evident that generally a relatively narrowband jammer has an advantage in jamming a DSSS receiver over a wideband jammer. For the jammer however the difficulty lies in knowing where to concentrate the narrowband signal to take advantage of this fact.

1. Jamming IEEE 802.11b

By examining Equation 5.4 one realizes that the one distinguishing design feature that results in the WLAN DSSS signal not displaying LPD characteristics is also a significant impediment to its ability to resist jamming. One of the most important variables when it comes to jam resistance in a DSSS system is the processing gain. System designers have direct control over processing gain and if given strict requirements for AJ performance processing gain would have to be increased. Unfortunately additional requirements usually translate to added complexity and additional costs. The developers of the 802.11 standard were guided by the requirement to operate in the ISM band while achieving a certain level of performance with an affordable design, and so that is where the baseline was set. In addition to limiting the maximum transmit power in the ISM band; the FCC requires that spread spectrum systems must achieve a minimum processing gain of 10 dB.

In addition to Equation 3.1, the following equation provides a very close approximation of a DSSS processing gain:

$$PG \cong 10\log K \qquad (5.5)$$

where K once again equals the number of bits in the spreading code. Equation 5.5 illustrates more clearly the direct impact of the length of the spreading sequence has on the processing gain. Besides the code length, there are other design features, such as error coding and antenna directivity, that can impact overall processing gain, but for the WLAN these features are nominal. See Figure 21 for a graphical illustration of the significance of the spreading code length in terms of system performance. This example illustrates a DSSS system using BPSK modulation. In one case the system employs a 127-bit maximal length sequence spreading code and in the second case a 15-bit sequence. Note that in both cases the system throughput remains constant at unity until reaching the respective AJ Margin for each case. As one would expect, and Figure 21 illustrates, the throughput for the system employing the 15-bit sequence drops off at a lower interference-to-signal ratio than does the 127-bit maximal sequence. [25]

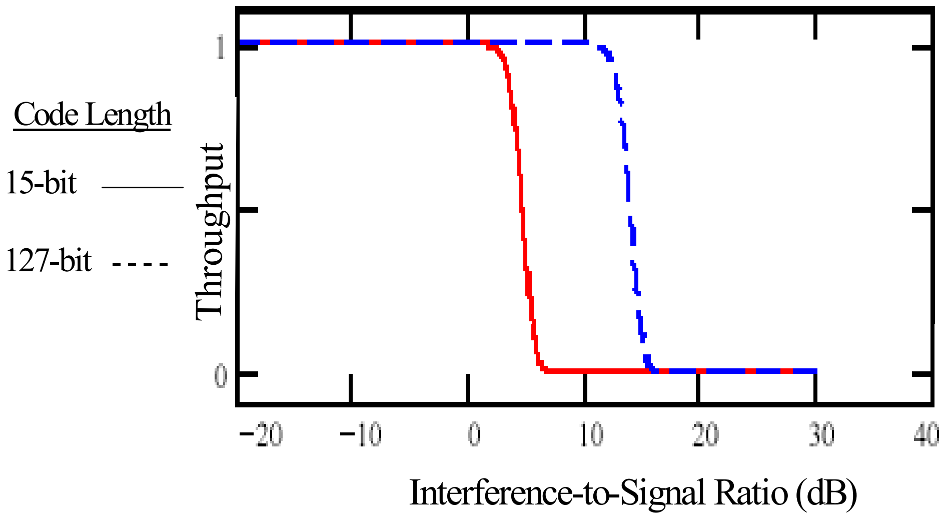

Figure 21. DSSS throughput vs. Interference-to-Signal Ratio [From: 25]

By using Equation 5.5 the processing gain for the two lengths of WLAN spreading codes is:

11-bit Barker code: $PG \cong 10\log(11) = 10.4dB$

8-bit CCK sequence: $PG \cong 10\log(8) = 9dB$

The first thing one should notice is that according to Equation 5.5 the 8-bit CCK sequence employed in the high-rate WLAN does not provide the FCC minimum 10dB of processing gain. During the development of the 802.11b standard the FCC allowed the designers to add 2dB of coding gain as a result of the employment of M-ary Orthogonal Keying (MOK). [24] This then gives an 11dB processing gain when using CCK sequences. With these processing gains we can determine the AJ Margin for both the low and high rate 802.11b signals. See Table 8 for a comparison of these AJ Margins.

	1Mbps 11-bit Barker	**11 Mbps 8-bit CCK**
PG	10.4dB	11dB
SNR	10.2dB (Fig 22)	16.8dB[From: 24]
RL (nominal)	2dB [From: 24]	2db [From: 24]
AJ Margin	-1.8dB	-7.8dB

Table 8. Comparison of 1Mbps and 11Mbps AJ Margins

Table 8 illustrates two critical points regarding the AJ characteristics of the 802.11b receivers; first that as a result of their minimal spreading codes their AJ capabilities are negligible, and secondly that the high rate signal is more easily interrupted than the low rate signal. This second point is further illustrated in Figure 22, which is a plot depicting percent of rate selection versus jamming-to-signal (J/S) ratio during a chamber test of a WLAN system. Recall that the 802.11b standard features automatic rate selection that enables the system to select the data rate based on the quality of the link between two stations. Notice in Figure 22 that at the lower J/S ratios the WLAN operates nearly one hundred percent of the time at 11 Mbps, but as the ratio increases the system switches to the lower rates until eventually the link deteriorates to the point that all communications cease. The system slowdown is noteworthy because often the jammer does not need to completely jam a receiver to be successful. A significant delay in traffic passing over the network, especially when transmitting video or graphic intensive traffic, might be sufficient.

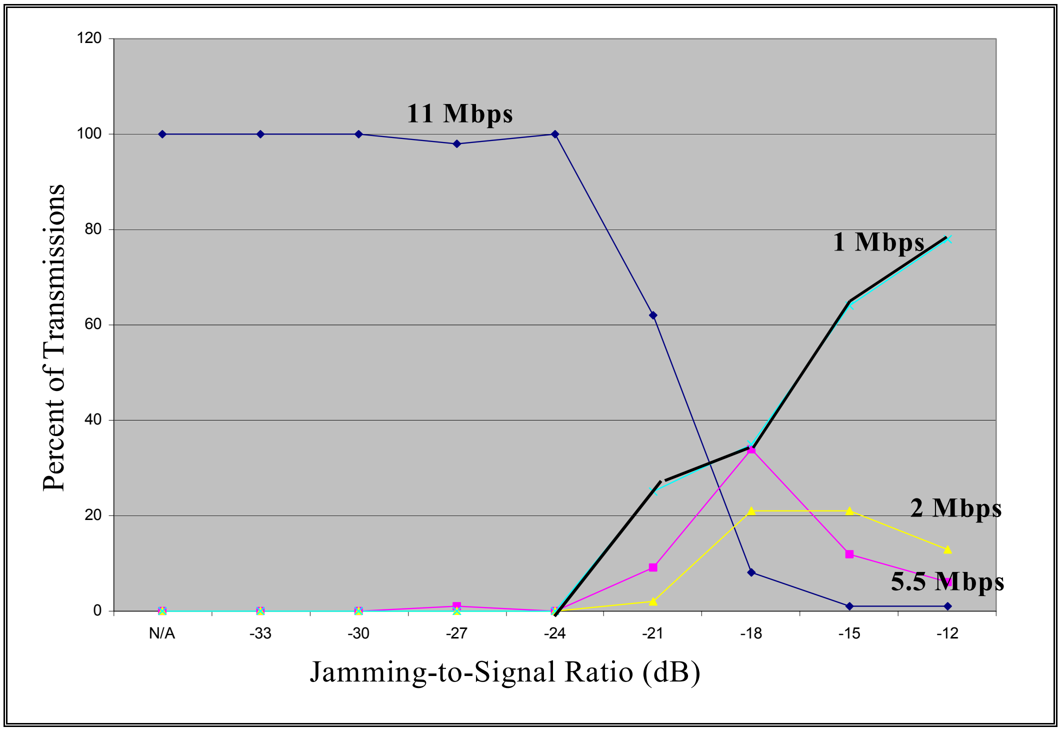

Figure 22. J/S vs. Data Rate [From: 25]

The minimal processing gain, and therefore AJ Margin, can be attributed once again to the reality that FCC compliance and interference rejection were the driving requirements when designing the PHY layer of the WLAN.

a. ELB WLAN

Because modifications to the PHY layer of the ELB WLAN are minimal, the previous discussion of 802.11b jamming is very significant. It is quite clear that the spread spectrum schemes employed in the 802.11b standard were not designed for a high threat EW environment that military unique communication systems usually are. This should be particularly evident when one realizes that a significant amount of research has been conducted just on the amount of interference a mere microwave oven has on a WLAN. As a result of this non-robust design any force choosing to employ this communication system in a tactical environment is certainly vulnerable to enemy jamming, even by an adversary of marginal technological means. As a follow-on to the LPD discussion, the one modification that has been made to the ELB WLAN that provides minimal AJ protection is the shift of the operating frequency from the ISM band. As opposed to jamming a commercial system, which can only be operating on one of 14 channels, an adversary would first have to find the operating frequency that the ELB force is employing. Once this is accomplished, however, the adversary should have little trouble jamming a WLAN station.

By understanding the characteristics of the ELB WLAN's PHY layer it is possible to predict how an adversary's jamming could have greatest detrimental impact upon the WARNET. As previously discussed, because of the significantly higher transmit power of the APs over the EUTs an adversary is most likely to initially detect the AP. But the higher power output is not the only basis for the APs increased vulnerability. In network terminology the topography of an infrastructure WLAN is that of a star network, meaning that one central hub controls all traffic. See Figure 23 for a depiction of the ELB star network topography. The central hub in the case of the ELB WLAN is the communications vehicle with an AP onboard; therefore all traffic must either originate at or be destined for the communications vehicle. For example, in Figure 23, if EUT #1 wants to communicate with EUT #2 it must first send the traffic to the AP, which will then relay the traffic to EUT #2. Because of this configuration, APs transmit much more frequently than the EUTs and are therefore more vulnerable to detection.

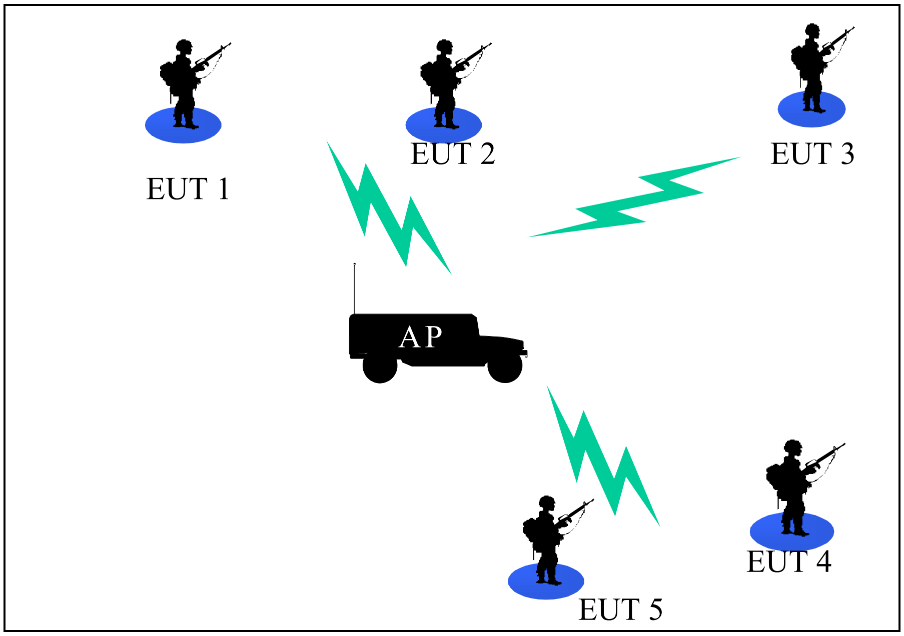

Figure 23. Star Topography

Not only are the APs more at risk to detection than the EUTs, but also because the EUTs are transmitting to them at a lower power (6W) level than they transmit back (30W), the APs are easier to jam. This is evident from Equation 5.4, where the output SNR is greater for the APs than the EUTs; therefore the receiver AJ Margin is lower for the APs. The combination of being quicker to detect and easier to jam could not be worse with regards to its implications for the network. Due to the WLAN's star topography, if the adversary is successful in jamming the AP then it has effectively jammed the entire BSS. As illustrated in Figure 23, EUTs 1 through 5 would no longer be able to communicate via the WLAN if the AP were jammed.

There are certainly operational measures that commanders can employ to make the previous basic scenario more complicated for the adversary. For example, as illustrated in Chapter IV, in addition to the tier 1 communication vehicles, APs are also present on the tier 2 aircraft. If an airborne platform were within range of the EUTs then the EUTs would automatically attempt association with that AP and disassociate with the station being jamming. There is little doubt that the jamming of an aircraft would be more difficult than that of a ground vehicle, especially for an adversary of limited technological means. But it is also true that the airspace over a battlespace is a complicated and sometimes platform-dense environment that may be further complicated with the injection of multiple communication UAVs. It is therefore questionable whether it is wise to rely upon additional platforms that may not always be available.

D. EXPLOITATION

It is certainly conceivable of instances where, the tactical situation depending, an adversary could gain valuable intelligence and therefore tactical advantage by not disrupting the WLAN signal at all, but rather allowing communications to continue and attempt to monitor network traffic. An obvious, but tactically significant, advantage of exploitation over jamming is the ability to remain covert. Once a force begins emitting an active jamming signal it seriously risks revealing its own position and losing any sense of surprise. Signal exploitation often provides longer-term benefits than that of merely jamming a receiver. The ability to simply monitor network traffic is itself a tremendous advantage, but taking it one step further and spoofing the network opens the door to greater possibilities of injecting false intelligence and going so far as crippling the larger network.

History provides countless examples where the injection of false intelligence was decisive in the outcome of a battle; one of the most recounted being in 1942 when the United States fed false information to the Japanese about conditions on Midway Island and watched their reaction to solidify that Midway was in fact the point of the Japanese's next offensive. While attempting to gain the advantage through the transmission of false information may not be a new phenomenon, the ability to directly cripple an adversary's larger communication systems most certainly is unique to post-information revolution era conflict. Where in the past the great majority of communication systems transferred information, either verbal or written, between humans; present day communications involves the transmission of digital bits between computer networks. And because these networks are part of larger networks it provides an opportunity for a carefully planned computer network attack to spread exponentially. The axiom that a chain is only as strong as its weakest link may very well hold true for computer networks, and if so we must realize that what we put out into the field could have drastic repercussions back at the command center, and possibly beyond.

1. IEEE 802.11b

A vast majority of the public research regarding WLAN vulnerabilities has focused first on the ability of an intruder to receive network packets and second on deciphering of the packets in order to read the network traffic. The fact that a commercial WLAN can only be operating on one of fourteen channels normally makes the task of determining the operating frequency a trivial matter. In fact, a recent article discussing the ease of detecting WLANs coined a new term known as “war driving”, in which “you take an 802.11b-equipped notebook, the right software and drive around scanning for 802.11b access points.” [26] So this quickly eliminates any privacy that spread spectrum technology can provide against an intruder with an 802.11b compliant “sniffer”. Recalling the privacy pyramid diagram (Figure 13), one notices that this still leaves authentication and WEP as a means of maintaining privacy for the WLAN. These two features however have been shown to have their weaknesses and as a result the privacy of all WLANs is seriously in doubt. The following is a brief overview highlighting the potential vulnerabilities associated with various authentication techniques and WEP that have been identified [27], [28], [29].

a. Authentication

As briefly described in Chapter III, in an infrastructure WLAN a station is always in one of three states with respect to an AP. Those states are; state 1, unauthenticated and unassociated; state 2, authenticated and unassociated; and state 3, authenticated and associated. Full communications between an AP and a station are only possible in state 3. Although reaching step 3 is a two-step process, authentication is actually the only point at which an AP can deny a station access to its BSS. This is because association is primarily a network management function to keep track of which BSS a station is associated with to ensure traffic destined for it is properly routed. Once a station has been properly authenticated it is just a matter of associating with an AP before the station has full access to the WLAN. Because the standard is not specific on the details to achieve authentication several methods are currently in use.

The default authentication protocol, as provided for in the standard, is known as Open System authentication. Open System authentication provides no security at all because an AP using this technique will authenticate anyone who requests it. During normal operations an AP constantly transmits a broadcast beacon that includes its service set identity (SSID) and an AP running as an Open System will automatically authenticate any station using the broadcast SSID in its authentication request. It is easy to see that Open System authentication is the least secure means of implementing station authentication. However, because it is the default setting, many unsuspecting administrators have failed to change this insecure mode of operation.

A second form of authentication is exemplified by ORiNOCO's proprietary access control mechanism called Closed Network. When Closed Network is enabled the AP no longer broadcasts a beacon with the SSID, rather in order for a station to authenticate with an AP it must have prior knowledge of the SSID and transmit it in the authentication request. Upon the AP's receipt of the proper SSID the station is authenticated and moves up to state 2. Because the SSID is not broadcast via a beacon, and the station must have prior knowledge of it to join a network, the SSID is essentially a password, or shared secret, for network access. The problem with using the SSID as a password is that it is included in the MAC management frame header that is often transmitted by both APs and stations during normal WLAN communications. Figure 24 is an illustration of the MAC management header; one can see that the SSID is part of the MAC management frame.

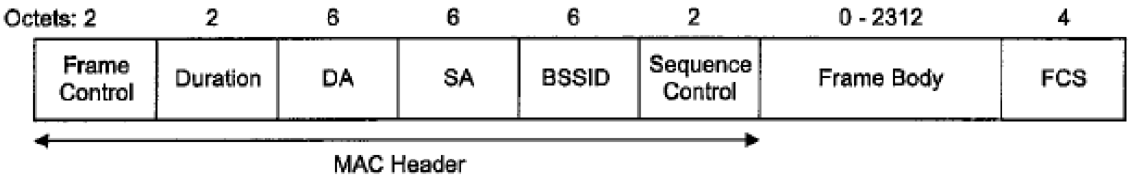

Figure 24. MAC Management Frame Format [From: 12]

To compound the insecurity, regardless of whether or not WEP in enabled, the MAC header is always transmitted unencrypted. So all an intruder needs to do is wait to intercept a management frame from either an AP or station, and then determine the SSID for use in his own authentication request. With the publication of this design flaw it became clear that this authentication mechanism is only marginally more secure than an Open System.

Another technique that is used by some vendors, but not defined in the standard, to provide security is the use of access control lists (ACL). In this scheme the AP is provided a list of MAC addresses that are permitted to access the network. When a station requests authentication the AP verifies whether the request is coming from a MAC address that is on the ACL; if it is then the station is authenticated, and if not access is denied. This method suffers from the same insecurity as the Closed Network scheme; the MAC addresses are part of the MAC management frames (Figure 24) that are routinely transmitted unencrypted by both APs and stations. Once a valid MAC address is "sniffed" an attacker can modify the MAC address of his wireless NIC to the valid one in order to gain access to the network.

The final, and certainly most secure means of authentication is the shared key method. This technique uses a challenge and response format along with a shared secret key to provide authentication. Under this method the AP, upon receiving a request for authentication, responds to the requesting station with an unencrypted challenge text. When the station receives the challenge it encrypts the challenge text using a pseudo-random sequence generated by a concatenation of a new initialization vector (IV) and the shared key and sends it back to the AP with the IV. Next the AP decrypts the received encrypted challenge using the shared key and the IV that was sent by the requesting station, and if the challenge text matches the one that was sent the station is authenticated. Although more secure than other methods, this technique is insufficient because if an intruder can copy the challenge request from the AP, with the unencrypted text, and the station's response, with the encrypted text and the IV, he then possesses enough information to determine the pseudo-random sequence used to encrypt that one particular message. With this piece of information he can now properly authenticate a challenge request from the AP without actually knowing the shared key.

After reviewing all the methods of authentication, and their associated weaknesses, it is clear that authentication is not a major obstacle for a determined attacker. Although a station may be successful in achieving authentication, it should be noted that an attacker should have to overcome additional security features to overcome in order to gain useful information from the WLAN. Only the most negligent of network administrators would operate a WLAN without employing WEP and higher-level protocols.

b. WEP

The final implementation in the privacy pyramid is the use of the WEP protocol. Recall that WEP was not designed to be the end-all in network security. As its name implies it was envisioned that it would provide a level of privacy for packets in transit equivalent to that of wired networks. There is without question a great dissimilarity in operating environments between wired and wireless networks. Where as eavesdropping in a wired network normally requires physically tapping into the network, in a wireless network it could be as easy as plugging a wireless NIC into a laptop computer and waiting. As such the fundamental goal of WEP is to prevent eavesdroppers from obtaining information from packets in transit. Its ability to achieve this goal however has been seriously called into question as a result of research conducted first at the University of California, Berkeley, and most recently, at AT&T Labs, Florham Park, New Jersey.

In both research efforts the teams showed that WEP's implementation of the RC4 cipher, specifically its use of an IV to generate the pseudo-random sequence, is flawed and subject to compromise. Recalling that it is a concatenation of the IV and the shared key that generates the pseudo-random sequence used for encryption, any reuse of the same combination of IV and shared key for subsequent messages results in encryption with an identical sequence. The serious implications of this detail are realized when one combines the fact that the shared keys are rarely changed and the IV is transmitted in the clear. This problem is further compounded by some implementations that result in the reuse of some IVs more often than others. For example, some PCMCIA cards reset the IV to zero each time they are reinitialized and then increment the IV by one for each transmitted packet. The result of this is that low-valued IVs are reused much more often than higher ones. Regardless of the IV generation scheme, because the IV field is only

24-bits wide it is inevitable that IVs will be reused. In fact it has been shown that a busy AP can exhaust all combinations of IVs within 12 hours.

Initial research focused on obtaining a plaintext copy, of an intercepted encrypted message to learn the encryption sequence associated with the IV employed and use that to decrypt other messages with the same sequence. This is similar to the technique used to defeat the shared key authentication scheme. In this case however the study went further to illustrate some active means of acquiring plain text copies of multiple messages in order to build up a library of sequences that could be later be used to decrypt messages. These attacks are fairly complicated and some rely upon the use of the Internet to build up information over a period of time. Whereas the Berkeley researchers relied upon a library of sequences to decrypt WEP messages, the AT&T researchers showed that by knowing only the initial part of an encrypted message they were able to actually decipher the secret key after only 15 minutes of monitoring WLAN traffic. This attack relies upon the fact that formatted traffic often contains the same first byte of information, that is used to let the receiving station know what protocol is being employed, as well as the exposed IV. This discovery goes much further than the previous findings because it is a completely passive operation that actually deciphers the secret key. As a result an attacker can decrypt traffic without actually having seen the sequence produced key-IV combination previously and can do so much quicker than previously thought. It is also important to note that this latest attack is just as effective against a 128-bit key as it is against a 40-bit key.

From the research being conducted on the WEP protocol it is apparent that it does not live up to its billing as providing privacy equivalent to wired networks. A review of the weaknesses associated with the three privacy mechanisms that the vendors tout leaves no doubt that if a WLAN is not employing some higher-level security protocols its traffic is essentially out in the open for any moderately determined attacker to see. In general this cannot be said for wired networks due to the difficulty of gaining physical access to the network.

2. ELB WLAN

There are no modifications to the ELB WLAN that alter its susceptibility to the previously discussed attacks. While there is no question that the disclosed weaknesses of the 802.11 authentication techniques and the WEP protocol should be of serious concern to the ELB program, it is also clear that the tactical battlespace environment may not be conducive to carrying out such attacks. Mobility, being one of the pillars of the OMFTS operational concept, may be one of its greatest assets in avoiding the described 802.11 exploitations. Virtually all of the attacks carried out in the previous research were conducted against fixed APs that operated in a fairly consistent, or predictable, manner. This is contrary to what one would expect from a mobile AP on the littoral battlespace. Intercepting the large number of packets required to carryout many of the discussed attacks would require an adversary maintain contact with an AP for potentially a considerable amount of time. Additionally, as was previously pointed out, the use of higher-level security protocols seriously impacts an attacker's ability to gain useful information from intercepted WLAN transmissions. Without question it would be more advantageous not to have to rely on the additional security protocols because they add additional overhead, but they are available and effective in avoiding the compromise of information. Another factor to consider regarding WEP is that a basic premise of both major studies is that the shared key is rarely changed. Whereas many civilian organizations with less experience in such matters may not be very familiar with sound security policies, operational military units routinely work with changing keys to maintain secure communications.

One fundamental WLAN implementation that does have potential to compromise tactical operations is the transmission of addresses in the clear. Without gaining any direct access to the network, an intruder within range of an AP has the ability to intercept packets that include the address of each EUT that is either receiving from or transmitting to the AP. This piece of information could enable an adversary to conduct network traffic analysis to determine the nature of the forces within the geographical range of the AP. If an adversary were able to combine the interception of unencrypted EUT addresses with an ability to authenticate with the AP he would have the means to conduct a DOS attack by constantly transmitting control frames, such as RTS/CTS, thereby preventing EUTs from gaining access to the medium.

a. EUT Capture

Perhaps the greatest source for potential exploitation of the WLAN is in fact not a direct product of the 802.11 standard at all. Because of the combination of additional security provided by higher-level encryption and the network operating system along with OMFTS mobility it is unlikely that an intruder will have the ability to directly inject false intelligence or malicious code. This however is not the case should a EUT fall into the hands of the enemy. Although certain measures are in place to protect the EUTs, such as hard drive encryption and terminal passwords, they would be insufficient to prevent exploitation should the EUT be captured while in use. In this situation the operator would have already entered his passwords for the actual terminal and the network operating system. Because at this junction the enemy has a fully authenticated EUT with all the required passwords entered, he now has the capability to reach back to the higher-level WARNET tiers and the potential to inject damage to the higher level networks, which would have a much greater impact than merely intercepting traffic. There is little doubt that the capture of communications gear has always been a consideration in combat, but the potential ramifications are much worse than ever before.

VI. CONCLUSION

A. SUMMARY OF VULNERABILITIES

As previously mentioned, system vulnerabilities in and of themselves should not be sufficient grounds to reject a communications system if it can be determined an adversary cannot reasonably exploit them, now or in the near future. Further, communication systems cannot be studied in a vacuum, for given enough time almost any potential enemy will be able to find holes in most systems. The anticipated tactical employment of a communications system must be the overriding consideration when determining whether the benefits of such a system outweigh the risks associated with the vulnerabilities. The adage that "perfection is the enemy of good enough" holds true for communication systems design. Rather than attempting to acquire the perfect system, which most likely does not exist, it is the program manager's responsibility to acquire one that meets the requirements, as proposed by the operational community.

With this frame of reference then, it is a worthwhile undertaking to try to evaluate the impact of the ELB WLAN potential vulnerabilities on the entire WARNET and ultimately on the communications aspect of the OMFTS. As addressed in Chapter V, the ELB WLAN is certainly not without vulnerabilities. Because the WLAN is based on the 802.11 standard, which only defines operations at the physical and MAC layers, the vulnerabilities explored were restricted to those two levels.

1. Physical Layer

There should be little question that the 802.11 standard physical layer is highly vulnerable to signal detection and interruption. A commercial standard designed to meet FCC regulatory restrictions and minimize ISM band interference; by military standards it produces a non-robust signal that could be a significant liability in almost any tactical situation. Although the vulnerabilities of the physical layer have not been publicly explored to the extent of those at the MAC layer, they may very well be the source of greatest risk when it comes to military utilization. Traditional EW techniques of detection, DF, and jamming of such a non-robust signal should prove effective and within the capabilities of almost any conceivable adversary. Although certain measures have been taken to modify the physical layer for ELB they are minimal at best.

2. MAC Layer

Although the very public MAC layer weaknesses related to inadequate authentication techniques and the WEP protocol should undoubtedly be a concern to the ELB program, in a tactical environment these longer-term weaknesses should take a back seat to the more near-term physical layer vulnerabilities. In fact if one could be confident that the physical layer was secure then the MAC layer vulnerabilities would be of little consequence. However, this is not the situation and so the vulnerabilities that are dependent on the MAC layer implementation features of the 802.11 standard could potentially be exploited by an adversary, but it seems apparent that higher level security protocols and procedures could minimize the extent of the compromise.

B. IMPACT OF ELB VULNERABILITIES ON OMFTS

OMFTS, as does JV 2010, places overwhelming emphasis on an unprecedented degree of dominate maneuver on the battlespace. The anticipated high tempo of combat operations will be carried out by lighter forces that will seek to exploit enemy weaknesses with the objective of dealing a decisive blow that should ultimately lead to victory. As made clear by then-Brigadier General Robert Shea in a statement before Congress in March 2000, the Marine Corps is reliant upon technological enhancements in the area of C2 systems to provide the additional speed and operational flexibility to make dominate maneuver a reality. [30] The C2 systems that General Shea was referring to are those that must provide small operational units a never before possible degree of SA while enabling those units to control the information they require.

Within the context of the ELB ACTD the WLAN is a critical component of the C2 system that General Shea spoke about before Congress, because it is the one means of communication amongst the units on the battlespace, as well as their link back to the command elements afloat. It is for this reason that an understanding of the WLAN's vulnerabilities is vital to the overall success of the ELB program. In particular the vulnerabilities associated with the non-robust physical layer of the WLAN are substantial and seriously call into question its suitability for use in the WARNET. The concept of dominant maneuver by small units with a high level of SA requires a new paradigm when it comes to communication systems. Traditionally, LPD communication systems have been generally reserved for the Special Forces who largely rely upon remaining covert to accomplish their mission. In many respects the small units that will be expected to carry out the operational missions envisioned by OMFTS will operate in modes previously reserved for reconnaissance and Special Force units. The OMFTS operational units will be lightly armored with a significantly reduced logistics infrastructure with which to support themselves. Rather than fight their way towards the objective, they will use their SA to avoid the enemy's strengths and attack them where they are weakest. And because they will be lightly armored they will call upon extremely responsive, accurate and lethal fire support from forces afloat. Their SA and calls for fire, however, are reliant upon a reliable means of communication. If the enemy is able to jam the central hub of their communication network, then these small units will be without the information required to maintain SA while at the same time being unable to call for fire support. Furthermore, because of the weak LPD characteristics of the WLAN signal, the very communications that they will rely upon for information could compromise their position and bring the enemy down upon them. It is highly questionable whether a Marine in the field will want to transmit via the WLAN if he believes his position may be compromised.

It is certainly no secret that various militaries throughout the world are experimenting with COTS-based wireless networks to support the next generation of operational concepts that all seem to place great emphasis on information superiority. Therefore it should also come as no surprise to learn of the resurgence of traditional EW systems, capable of signal detection, DF, and communications jamming. Therefore if the Marine Corps should decide to continue with a COTS-based solution, such as the 802.11b standard, it must be anticipated that a potential adversary will be well prepared with sufficient EW systems and a good understanding of the underlying technology behind the communications network. Given this inevitability it is imperative that a robust RF signal, displaying LPD and anti-jam characteristics, be employed to ensure the units that will carry out OMFTS operations have a reliable means of communications to enable dominant maneuver on the littoral battlespace.

At this point in time, the impact of the MAC layer security vulnerabilities appears to be almost negligible when compared to those of the physical layer. The time requirements associated with exploiting the disclosed vulnerabilities are too long to reasonably take advantage of during high-tempo operations where information is perishable. Should however the WLAN be employed during a protracted operation, such as a peacekeeping mission, where a unit's position may remain fixed for prolong periods of time it is conceivable that an adversary could exploit the MAC layer vulnerabilities.

C. RECOMMENDATIONS

While it seems almost certain that there is a valid requirement for wireless networking on the future battlefield, the technology that will turn this requirement into reality is less clear. Although the third generation of wireless products has already hit the market place, wireless networking is far from a mature technology. Rapid advancements continue to push the limits of wireless throughput, for example the 54Mbps IEEE 802.11a standard is just now beginning to gain acceptance in the commercial sector. The problem for the military sector however is that the prime motivation for private sector wireless research is the desire for more throughput and not necessarily security, certainly not security in the military sense anyway. This schism is particularly difficult to balance during an era where the emphasis is on achieving interoperability and competitive pricing by adopting COTS products for military systems. For mission critical military communication systems security cannot be an afterthought, as it sometimes appears it is in the commercial sector. No mater how much throughput a wireless network can produce, it will do the user no good whatsoever if the enemy can easily interrupt it, either through DF techniques and/or jamming. The competing priorities between the commercial and military sectors are nowhere more divergent than at the physical layer of the wireless network. Where the commercial sector benefits from a well defined, easy to implement standard that is cost effective while at the same time satisfying regulatory requirements, the military sector benefits from a robust signal that is difficult for an enemy to detect and interrupt.

Because of the divergent requirements the DoD must seek alternate solutions for wireless network physical layer implementations. The operational concepts of high-tempo operations, conducted by dispersed units relying upon information superiority over the enemy, demand reliable communications that can go undetected and undisturbed. This requirement cannot be satisfied by a commercial standard. It could, however, be satisfied by a spread spectrum system that incorporates true transmission security characteristics, such as DSSS with maximal codes, or a hybrid DSSS-FHSS system. Another alternative that is not new to military communications, and is also gaining acceptance in the commercial sector, is the utilization of an ultra-wideband (UWB) communication system. Displaying strong LPD characteristics, UWB radios have generally been used by special operations units. In the past UWB communications have been limited by slow data rates and short ranges, but as illustrated in Figure 25 there have been significant improvements in both these areas and the forecast is for the trend to continue.

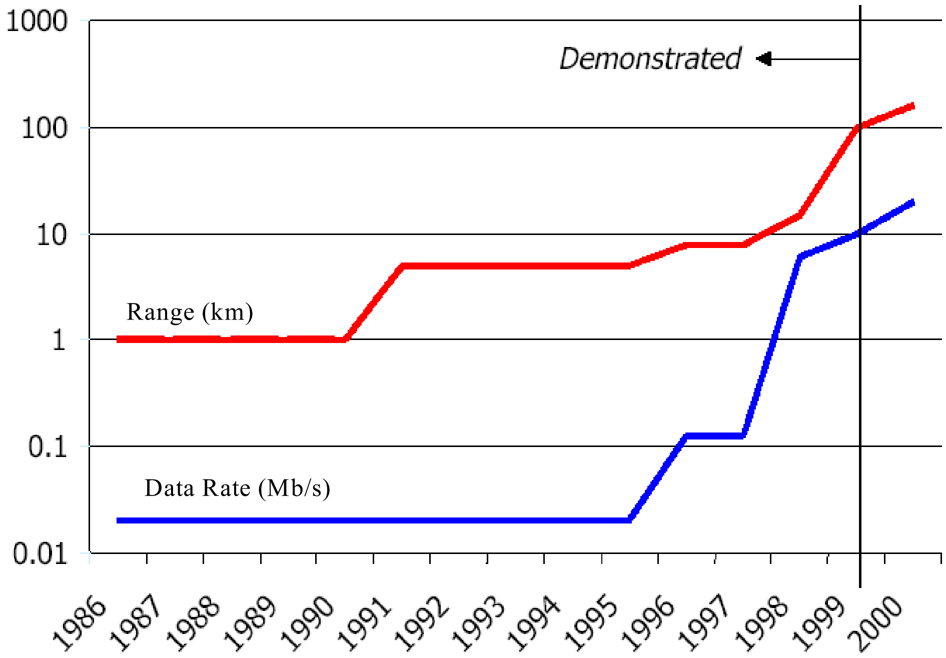

Figure 25. UWB Advances [From: 31]

Although both the robust spread spectrum and UWB solutions would probably translate, at least in the short-term, into lower throughput this should be an acceptable consequence of obtaining a more secure physical layer. While there is little question that there will always be a desire on the part of operational community for additional throughput, the reality is that if properly managed a lower throughput, but more robust network will better meet the requirements of the operating units. For example, the desire to conduct video teleconferences (VTC) over the WARNET turns out to be one of the most bandwidth intensive applications for the ELB WLAN. Rather than transmitting the VTC down to the smaller units on tier 1 communications systems, it may be better to limit the VTC to units capable of communicating via tier 2 or tier 3 systems. While it may be nice to conduct a VTC with one of the small dismounted units, it is doubtful that this additional capability is worth the insecurity associated with a system capable of making it a reality. Additionally, while the more secure solutions would undoubtedly prove more expensive than the cost-effective 802.11b systems, once again the security benefits gained should more than outweigh the costs. If the transformation of operational concepts is going to based on the additional access to information made possible by technological advances during the information revolution, then it vital that the communication systems upon which the exchange of information is dependent receive the appropriate priority and not be relegated as a support function.

The physical security of wireless EUTs is another area in which additional measures must be considered to improve the security of the entire network. Passwords and hard-drive encryption are a good start and should be part of a defense-in-depth solution, but alone they are not enough. This is one area of wireless network security that has seen considerable interest in the commercial sector and for this reason the solutions should be fairly easy to implement. The incorporation of biometrics to authenticate the user to the EUT is one feature that could prevent its use by unauthorized personnel. Unlike a password however, it should not be a one-time authentication process rather it should be a continuous authentication process that if interrupted ceases operation of the EUT. A second feature that would contribute to security is the ability to destroy the terminal via remote means should it fall into enemy hands. This feature is gaining widespread acceptance in the commercial sector where the problem of stolen laptop computers is a significant obstacle in maintaining a competitive market advantage.

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

1. The Information Warfare Site, “RMA & C4I,” URL: [http://www.iwar.org.uk/rma/index.htm], no date.

2. Metz, Steven and Kievit, James, *STRATEGY AND THE REVOLUTION IN MILITARY AFFAIRS: From Theory to Policy*, U.S. Army War College, June 1995.

3. Parker, Michael and Arp, Lance, *Scalability Study of Wireless Tactical Communication in Support of a Marine Corps Expeditionary Brigade*, Master’s Thesis, Naval Postgraduate School, Monterey, California, June 2000.

4. Survivability and Lethality Analysis Directorate, “Vulnerability Analysis”, URL: [http://web.arl.mil], no date.

5. “…From the Sea”, URL: [http://www.nwdc.navy.mil/Products/Library/documents/fts.asp], September 1992.

6. U.S. Department of Defense, *OPERATIONAL MANEUVER FROM THE SEA*, Government Printing Office, D.C., 1997.

7. U.S. Department of Defense, *JOINT VISION 2010*, Government Printing Office, D.C., 1996.

8. LtGen Paul K. Van Riper statement to the Procurement Subcommittee and Research and Development Subcommittee of the House National Security Committee, “Information Superiority”, URL: [http://www.comw.org/rma/fulltext/infosup.html], June 1997.

9. “Introduction to ACTDs” URL: [http://www.acq.osd.mil/actd/intro.htm], May 2001.

10. “Department of the Navy Acquisition Reform Specifications and Standards Reform Initiative”, URL: [http://www.acq-ref.navy.mil/pdf/implman.pdf], April 1998.

11. Anderson, Robert and Hundley, Richard, “The Implications of COTS Vulnerabilities for the DoD and Critical U.S. Infrastructures: What Can/Should the DoD Do?”, RAND, 1998.

12. O'Hara, Bob and Petrick, Al, "IEEE 802.11 Handbook: A Designer's Companion" IEEE Press, New York, NY, 1999.

13. Intelligrahics Corporation, "Introduction to IEEE 802.11" URL: [http://www.intelligraphics.com/articles/802.11_article.html], no date.

14. Geier, J., *Implementing Interoperable Networks,* MacMillan Technical Publishing, New York, NY, 1999.

15. 3com Corporation, "IEEE 802.11b Wireless LANs", URL: [http://www.3com.com/other/pdfs/infra/corpinfo/enUS/50307201.pdf], April 2000.

16. Intersil Corporation, "A Condensed Review of Spread Spectrum Techniques for ISM Band Systems", URL: [http://www.intersil.com/data/an/an9/an9820/AN9820.pdf], May 2000.

17. Althouse, Edwin L. , "Extending the Littoral Battlespace (ELB): Advanced Concept Technology Demonstration (ACTD)", June 1999.

18. Costello, Brian, "ELB MSD-2 Communications Architecture Brief", January 2001.

19. Borden, Andrew "What is Information Warfare?" URL: [http://www.airpower.maxwell.af.mil/airchronicles/cc/borden.html] November 1999.

20. Russell, Steve F. "Wireless Channel Security Tutorial", URL: [http://www.public.iastate.edu/~sfr/wireless/w_tut_1.html], February 1997.

21. Direct Network Services Corporation, "Wireless LAN Security", URL: [http://www.directnetserv.com/security.htm], no date.

22. Nicholson, David L., *Spread Spectrum Signal Design: LPE and AJ Systems*, Computer Science Press, 1988.

23. FBIS Reports, "Indian Troops Eliminate Seven Pakistani militants in single encounter in Kashmir", April 2001.

24. Andren, Carl and Webster, Mark, “CCK Modulation Delivers 11Mbps for High Rate IEEE 802.11 Extension”, URL: [http://www.intersil.com], November 2000.

25. McCune, Earl, “An Impartial Comparison of Direct-Sequence and Frequency-Hopping Spread Spectrum Performance with ISM-Band Narrowband Interference”, URL: [http://www.tropian.com/tech/tech_docs/sscompare.pdf], no date.

26. Santalesa, Rich, “The War Over 802.11x Security”, URL: [http://techupdate.zdnet.com/techupdate/stories/main/0,14179,2783681,00.html], July 2001.

27. Arbaugh, William and Shankar, Narendar, “Your 802.11 Wireless Network has No Clothes” URL: [http://www.cs.umd.edu/~waa/wireless.pdf], March 2001.

28. Borisov, Nikita and Wagner, David, “Intercepting Mobile Communications: The Insecurity of 802.11”, URL: [http://www.cs.berkeley.edu/~daw/papers/wep-mob01.pdf], no date.

29. Stubblefield, Adam and Rubin, Aviel, “Using the Fluhrer, Mantin, and Shamir Attack to Break WEP” , URL: [http://www.info-sec.com/crypto/01/crypto_080701a_j.shtml],August 2001.

30. Statement of Brigadier General Robert M. Shea to the House Military Readiness and Military Research & Development Subcommittees, “Information Superiority and Information Assurance”, March 2000.

31. Multispectral Solutions Corporation, “Recent Applications of Ultra Wideband Communications and Radar Systems”, December 2000.

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Fort Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California

3. Professor John Osmundson
   Naval Postgraduate School
   Monterey, California
   josmundson@nps.navy.mil

4. Lieutenant Commander Raymond Buettner
   Naval Postgraduate School
   Monterey, California
   rrbuettn@nps.navy.mil

5. Commander John P. O'Sullivan
   Commander, Carrier Group TWO
   NS Norfolk, Virginia
   osullijp@ccg2.navy.mil

6. Lieutenant Colonel Brian Costello
   Office of Naval Research
   Arlington, Virginia
   costelb@onr.navy.mil

7. Mr. Roberto Sandoval
   Joint Information Operation Center
   Lackland AFB, Texas
   robert.sandoval@jioc.osis.gov

8. Director, Marine Corps Research Center, MCCDC, Code C40RC
   Quantico, Virginia
   ramkeyce@tecom.usmc.mil
   strongka@tecom.usmc.mil
   sanftlebenka@tecom.usmc.mil

9. Professor Dan C. Boger
   Naval Postgraduate School
   Monterey, California
   dcboger@nps.navy.mil